

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-055961

(43)Date of publication of application : 20.02.2002

(51)Int.Cl.

G06F 15/00

B42D 15/10

G06K 17/00

G06K 19/07

G09C 1/00

(21)Application number : 2000-245818

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 14.08.2000

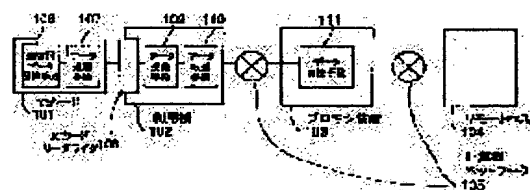
(72)Inventor : INOUE KAZUNORI  
SAKUSHIMA KAZUO  
TANABIKI MASAKI  
KIKUCHI TAKAFUMI

## (54) IC CARD DEVICE AND PROXY DEVICE, AND CARD TERMINAL DEVICE

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To allow an IC card system to make access destination information, etc., secret to a used machine and also prevent the secret information from leaking from the used machine when the security of the used machine is not high enough.

**SOLUTION:** This IC card system is equipped with an IC card 101, the used machine 102 which is connected by a computer network 105, a proxy device 103, and a remote host 104. When network service is received by accessing the remote host 104 by using the IC card 101, the IC card 101 and proxy device 103 communicate with each other. At this time, an application program on the IC card 101 and a data converting means 111 of the proxy device 103 settle a rule and a method for data conversion and the used machine 102 performs data conversion by unknown conversion algorithm to send and receive data. Consequently, information can be kept secret to the used machine 102 and its disclosure can be limited.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of



## 【特許請求の範囲】

【請求項 1】 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行う IC カードシステム用の IC カード装置であって、

送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段とを備え、前記カード端末装置と計算機ネットワークを介して接続されたリモートホストとデータ通信を行う際に、このリモートホストと前記カード端末装置との間に設けられるプロキシ装置と当該 IC カード装置との間で予め定めたものであって、かつ、前記カード端末装置には未知のものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するためのデータを前記プロキシ装置へ送信することを特徴とする IC カード装置。

【請求項 2】 前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を、前記カード端末装置が解釈困難なキーデータとして生成する通信キーデータ生成手段を備え、前記変換アルゴリズムもしくは変換パラメータとして、当該 IC カード装置と前記プロキシ装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いてデータ変換処理を実行する際に、前記通信キーデータを前記プロキシ装置へ送信することを特徴とする請求項 1 記載の IC カード装置。

【請求項 3】 通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記プロキシ装置または前記リモートホストとの間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成することを特徴とする請求項 1 記載の IC カード装置。

【請求項 4】 前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記プロキシ装置との間で形成したセキュアパスを経由して該プロキシ装置へ送ることを特徴とする請求項 3 記載の IC カード装置。

【請求項 5】 前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順を異なる鍵情報を用いることによりデータの暗号化を行う第 2 の暗号処理手段を備え、前記第 2 の暗号処理手段により当該 IC カード装置が保持する任意のデータを暗号化し、この第 2 の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第 2 の暗号化データを前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送ることを特徴とする請求項 4 記載の IC カード装置。

【請求項 6】 前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順

を異なる鍵情報を用いることによりデータの暗号化を行う第 2 の暗号処理手段を備え、

前記第 2 の暗号処理手段により当該 IC カード装置が保持する任意のデータを暗号化し、この第 2 の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第 2 の暗号化データを前記リモートホストのアクセス先情報の暗号化データと共に前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送ることを特徴とする請求項 4 記載の IC カード装置。

【請求項 7】 当該 IC カード装置と前記プロキシ装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成することを特徴とする請求項 3～6 のいずれかに記載の IC カード装置。

【請求項 8】 当該 IC カード装置と前記プロキシ装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパスを形成することを特徴とする請求項 3～6 のいずれかに記載の IC カード装置。

【請求項 9】 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行う IC カードシステム用の IC カード装置であって、

送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置において実現するユーザインタフェースに関わる UI リクエスト情報を、このカード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置に送信する UI リクエスト情報送信手段とを備えたことを特徴とする IC カード装置。

【請求項 10】 前記 UI リクエスト情報として、文字コードに関わる文字列情報を用いることを特徴とする請求項 9 記載の IC カード装置。

【請求項 11】 前記 UI リクエスト情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させるためのプログラム情報による動作結果に影響を与えるパラメータ情報を用いることを特徴とする請求項 9 記載の IC カード装置。

【請求項 12】 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行う IC カードシステム用の IC カード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置の認証を行う端末認証手段と、前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、

前記カード端末装置が接続された計算機ネットワーク上

において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記プロキシ装置へ送ることを特徴とするＩＣカード装置。

【請求項１３】 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、

前記カード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記プロキシ装置から前記カード端末装置の信頼度評価結果を受け取ることを特徴とするＩＣカード装置。

【請求項１４】 前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えることを特徴とする請求項１２または１３に記載のＩＣカード装置。

【請求項１５】 前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対してＩＣカード装置から送信する情報の一部もしくは全てを削除もしくは変更することを特徴とする請求項１４に記載のＩＣカード装置。

【請求項１６】 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該ＩＣカード装置が保持する機密情報に関わる情報を削除もしくは変更することを特徴とする請求項１５に記載のＩＣカード装置。

【請求項１７】 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該ＩＣカード装置が保持するＩＣカードユーザのプライバシーに関わる情報を削除もしくは変更することを特徴とする請求項１５記載のＩＣカード装置。

【請求項１８】 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うＩＣカードシステム用のＩＣカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置と計算機ネットワークを介して接続されたリモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報

変換手段とを備え、

前記機密情報変換手段は前記カード端末装置より入力された第１の機密情報データを当該カード端末装置に対して秘匿性を持った第２の機密情報データに変換し、この第２の機密情報データを前記カード端末装置と前記リモートホストとの間に設けられるプロキシ装置へ送ることを特徴とするＩＣカード装置。

【請求項１９】 前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じてＩＣカードユーザに提示し、前記カード端末装置より入力された第１の機密情報データから前記変換キーデータを用いて前記第２の機密情報データを生成することを特徴とする請求項１８記載のＩＣカード装置。

【請求項２０】 前記変換キーデータと前記第１の機密情報データとを一対一に対応させて同一の第２の機密情報データを生成するための異なるデータの組を複数設けたことを特徴とする請求項１９記載のＩＣカード装置。

【請求項２１】 前記カード端末装置において実現するユーザインタフェースに関わるＵＩリクエスト情報を前記プロキシ装置に送信するＵＩリクエスト情報送信手段を備え、

前記ＵＩリクエスト情報として、前記リモートホストから要求される機密情報として前記第２の機密情報データの代わりに前記第１の機密情報データを入力すべきことをＩＣカードユーザに指示するためのＵＩ部品情報を用いることを特徴とする請求項１８～２０のいずれかに記載のＩＣカード装置。

【請求項２２】 予め定めた規則に従って計算機ネットワーク上の複数のプロキシ装置の中から一つを選択するプロキシ選択手段を備えたことを特徴とする請求項１～２１のいずれかに記載のＩＣカード装置。

【請求項２３】 前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置を逐次的に検索して選択することを特徴とする請求項２２記載のＩＣカード装置。

【請求項２４】 前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置をランダムに検索して選択することを特徴とする請求項２２記載のＩＣカード装置。

【請求項２５】 前記プロキシ選択手段は、前記カード端末装置に問い合わせ使用に適するプロキシ装置を選択することを特徴とする請求項２２記載のＩＣカード装置。

【請求項２６】 使用に適するプロキシ装置を選択するためのプロキシ装置のリストを有し、このリスト内容の追加、変更、削除の少なくともいずれか一つを行うプロキシ情報操作手段を備えたことを特徴とする請求項２２記載のＩＣカード装置。

【請求項２７】 前記カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態

を電子情報のやりとりによって生じさせるインセンティブを発行するインセンティブ発行手段を備え、このインセンティブに関する情報を前記カード端末装置との間で通信することを特徴とする請求項 1～26 のいずれかに記載の IC カード装置。

【請求項 28】 前記インセンティブとして広告情報を用い、前記インセンティブ発行手段は前記カード端末装置からこの広告情報を受信することを特徴とする請求項 27 記載の IC カード装置。

【請求項 29】 前記インセンティブとして金銭あるいは有価価値物に関連した有価価値電子情報を用い、前記インセンティブ発行手段はこの有価価値電子情報を前記カード端末装置に送信することを特徴とする請求項 27 記載の IC カード装置。

【請求項 30】 IC カード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる IC カードシステム用のプロキシ装置であって、前記 IC カード装置と当該プロキシ装置との間で予め定めたものであって、かつ、前記カード端末装置には未知のものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するデータ変換手段を備えたことを特徴とするプロキシ装置。

【請求項 31】 前記データ変換手段は、前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を前記カード端末装置が解釈困難なキーデータとして生成した通信キーデータを変換するもので、前記変換アルゴリズムもしくは変換パラメータとして、当該プロキシ装置と前記 IC カード装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いて変換処理を行うことを特徴とする請求項 30 記載のプロキシ装置。

【請求項 32】 通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記 IC カード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成することを特徴とする請求項 30 記載のプロキシ装置。

【請求項 33】 前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記 IC カード装置との間で形成したセキュアパスを経由して該 IC カード装置から受け取ることを特徴とする請求項 32 記載のプロキシ装置。

【請求項 34】 当該プロキシ装置と前記 IC カード装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成することを特徴とする請求項 32 または 33 に記載のプロキシ装置。

【請求項 35】 当該プロキシ装置と前記 IC カード装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパス

を形成することを特徴とする請求項 32 または 33 に記載のプロキシ装置。

【請求項 36】 IC カード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる IC カードシステム用のプロキシ装置であって、前記カード端末装置において実現するユーザインタフェースに関わる UI リクエスト情報を受信する UI リクエスト情報受信手段と、

前記受信した UI リクエスト情報の内容に基づいて前記カード端末装置におけるユーザインタフェース部品に関わる UI 情報を前記カード端末装置に送信する UI 情報送信手段とを備えたことを特徴とするプロキシ装置。

【請求項 37】 前記 UI 情報として、文字フォントに関わる文字画像情報を用いることを特徴とする請求項 36 記載のプロキシ装置。

【請求項 38】 前記 UI 情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用いることを特徴とする請求項 36 記載のプロキシ装置。

【請求項 39】 前記 UI 情報として、前記カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いることを特徴とする請求項 38 記載のプロキシ装置。

【請求項 40】 IC カード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる IC カードシステム用のプロキシ装置であって、前記カード端末装置の認証を行う端末認証手段と、前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記 IC カード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記 IC カード装置へ送ることを特徴とするプロキシ装置。

【請求項 41】 IC カード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる IC カードシステム用のプロキシ装置であって、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記 IC カード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記 IC カード装置から前記カード端末装置の信頼度評価結果を受け取ることを特徴とするプロキシ装置。

【請求項 4 2】 前記端末認証手段と前記端末信頼度評価手段の少なくとも一方が、前記カード端末装置の計算機ネットワークへの接続に関わる固有かつ一意の情報をを用いて動作することを特徴とする請求項 4 0 記載のプロキシ装置。

【請求項 4 3】 前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えることを特徴とする請求項 4 0 または 4 1 に記載のプロキシ装置。

【請求項 4 4】 前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対してプロキシ装置から送信する情報の一部もしくは全てを削除もしくは変更することを特徴とする請求項 4 3 記載のプロキシ装置。

【請求項 4 5】 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持する機密情報に関わる情報を削除もしくは変更することを特徴とする請求項 4 4 記載のプロキシ装置。

【請求項 4 6】 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持する IC カードユーザまたはプロキシユーザのプライバシーに関わる情報を削除もしくは変更することを特徴とする請求項 4 4 記載のプロキシ装置。

【請求項 4 7】 前記カード端末装置において実現するユーザインタフェース部品に関わる UI 情報を前記カード端末装置に送信する UI 情報送信手段を備え、前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対してプロキシ装置から UI 情報を送信する前に、前記 UI 情報の中から機密情報表示に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後の UI 情報を前記カード端末装置へ送ることを特徴とする請求項 4 4 記載のプロキシ装置。

【請求項 4 8】 前記カード端末装置において実現するユーザインタフェース部品に関わる UI 情報を前記カード端末装置に送信する UI 情報送信手段を備え、前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対してプロキシ装置から UI 情報を送信する前に、前記 UI 情報の中から機密情報入力に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後の UI 情報を前記カード端末装置へ送ることを特徴とする請求項 4 4 記載のプロキシ装置。

【請求項 4 9】 IC カード装置とデータのやり取りを

行うカード端末装置とこれに計算機ネットワークを介して接続されリモートホストとの間に設けられる IC カードシステム用のプロキシ装置であって、前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報変換手段を備え、前記機密情報変換手段は前記カード端末装置より入力された第 1 の機密情報データを当該カード端末装置に対して秘匿性を持った第 2 の機密情報データに変換し、この第 2 の機密情報データを前記リモートホストへ送ることを特徴とするプロキシ装置。

【請求項 5 0】 IC カード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されリモートホストとの間に設けられる IC カードシステム用のプロキシ装置であって、前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報に関して、前記カード端末装置より入力された第 1 の機密情報データが当該カード端末装置に対して秘匿性を持った状態に変換された第 2 の機密情報データを、前記 IC カード装置から受け取って前記リモートホストへ送る機密情報獲得手段を備えたことを特徴とするプロキシ装置。

【請求項 5 1】 前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じて IC カードユーザに提示し、前記カード端末装置より入力された第 1 の機密情報データから前記変換キーデータを用いて前記第 2 の機密情報データを生成することを特徴とする請求項 4 9 記載のプロキシ装置。

【請求項 5 2】 前記変換キーデータと前記第 1 の機密情報データとを一对一に対応させて同一の第 2 の機密情報データを生成するための異なるデータの組を複数設けたことを特徴とする請求項 5 1 記載のプロキシ装置。

【請求項 5 3】 前記カード端末装置において実現するユーザインタフェース部品に関わる UI 情報を前記カード端末装置に送信する UI 情報送信手段を備え、前記 UI 情報として、前記リモートホストから要求される機密情報として前記第 2 の機密情報データの代わりに前記第 1 の機密情報データを入力すべきことを IC カードユーザに指示するための UI 部品情報を用いることを特徴とする請求項 4 9 ～ 5 2 のいずれかに記載のプロキシ装置。

【請求項 5 4】 IC カード装置とデータのやり取りを行う IC カードシステム用のカード端末装置であって、当該カード端末装置は計算機ネットワーク上において設けられるプロキシ装置と接続され、前記プロキシ装置から送られた当該カード端末装置におけるユーザインタフェース部品に関わる UI 情報を受信する UI 情報受信手段と、前記受信した UI 情報の内容に基づいて前記 IC カード装置とのデータ通信に関するユーザインタフェースを実

10

20

30

40

50

行するUI実行手段とを備えたことを特徴とするカード端末装置。

【請求項55】 前記UI情報として、文字フォントに関わる文字画像情報を用いることを特徴とする請求項54記載のカード端末装置。

【請求項56】 前記UI情報として、当該カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用いることを特徴とする請求項54記載のカード端末装置。

【請求項57】 前記UI情報として、当該カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いることを特徴とする請求項56記載のカード端末装置。

【請求項58】 ICカード装置とデータのやり取りを行うICカードシステム用のカード端末装置であって、当該カード端末装置は計算機ネットワーク上において設けられる複数のプロキシ装置と接続され、前記ICカード装置からの問い合わせに応じて、予め定めた規則に従って使用に適するプロキシ装置を選択するための処理を行うプロキシ選択処理手段を備えたことを特徴とするカード端末装置。

【請求項59】 当該カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態を電子情報のやりとりによって生じさせるインセンティブを受けるインセンティブ獲得手段を備え、このインセンティブに関する情報を前記ICカード装置との間で通信することを特徴とする請求項54～58のいずれかに記載のカード端末装置。

【請求項60】 前記インセンティブとして広告情報を用い、前記インセンティブ獲得手段はこの広告情報を前記ICカード装置に送信することを特徴とする請求項59記載のカード端末装置。

【請求項61】 前記インセンティブとして金銭あるいは有価価値物に関連した有価価値電子情報を用い、前記インセンティブ獲得手段は前記ICカード装置からこの有価価値電子情報を受信することを特徴とする請求項59記載のカード端末装置。

【請求項62】 請求項1～29のいずれかに記載のICカードシステム用のICカード装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【請求項63】 請求項30～53のいずれかに記載のICカードシステム用のプロキシ装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【請求項64】 請求項54～61のいずれかに記載のICカードシステム用のカード端末装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカードシステムを構成するのに好適なカード本体を含むICカード装置、及びこのICカードと接触又は非接触でデータ通信を行うカード端末装置、並びにこのカード端末装置とネットワークを介して接続されるリモートホストとの間に設けてICカード装置とリモートホストの両者に対してデータ通信を行うプロキシ装置に関する。

10 【0002】

【従来の技術】一般に知られるICカードシステムは、図35に示すように、半導体記憶媒体を含むカード本体であるICカード51、カード端末装置である利用機（ICカード利用機）52、利用機52に対して情報の提供等を行うリモートホスト（ホストコンピュータ）53から構成される。利用機52は、リーダライタ55と端末56からなり、端末56はリーダライタ55を介してICカード51とデータ送受信を行う。さらに、端末56はネットワーク54を介してリモートホスト53ともデータ送受信を行う。リーダライタ55は、ICカード51に対し電源、クロックを提供するが、その際、接触端子を用いて電氣的に伝達する方法と、電磁波を用いて伝達する方法とがあり、それぞれ接触型、非接触型と呼ばれる。ICカード51それ自体は通常はユーザインタフェースを持たず、暗証入力、処理選択、表示等の機能は利用機52が担う。

【0003】ICカードの利点は、ICカードに内蔵されるICチップの対タンパ性（物理的、化学的、電氣的手段等によりICチップ内部状態の解析や改竄を試みる不正行為からICチップ内部の情報を保護する能力）に優れることである。さらに、ICカードの中でマイコンカードに分類されるものの多くは、ICチップ内で暗号処理（データを暗号アルゴリズムと鍵を用いて解読困難な状態に変換する処理）が可能となっており、電子商取引等の高いセキュリティが求められる分野での利用に適する。

【0004】計算機ネットワークにおいて暗号処理機能を有するICカードを利用する技術は、特開平4-35538号公報（暗号化通信方式、以下従来例1とする）、特開平4-326442号公報（メッセージ認証システム、従来例2）、特開平5-110873号公報（暗号機能通信システム、従来例3）に示されている。これらはいずれも計算機ネットワークに接続された利用機にICカードを接続し、ICカードが内部にも暗号処理機能を用いてネットワーク上で送受するデータの秘匿及び認証を行うものである。

【0005】ICカードのもう一つ利点は可搬性の高さである。この性質を利用し、ユーザ自身の固有情報を格納したICカードを訪問先の端末で使用する技術は、特開平7-306831号公報（コンピュータネットワー

クシステム、従来例4)、特開平10-21301号公報(地域保険医療情報システム及びこれに用いる可搬型記憶媒体、従来例5)、特開平11-15927号公報(ICカードシステム、従来例6)に示されている。これらの技術によれば、計算機ネットワーク上の複数の場所から共通のユーザ環境を得たり、一貫したサービスを受けたりすることができる。

【0006】また近年では、ICカードに内蔵されるICチップの性能の向上(処理速度、記憶容量の向上)とソフトウェア技術の向上(マルチアプリケーション環境の実現、仮想マシンによるソフトウェア不正動作の防止、カード発行後のアプリケーションダウンロード等)に伴い、より高機能、多用途、複雑なアプリケーションプログラムをICカード上で動作させることが可能になっている。

【0007】

【発明が解決しようとする課題】従来の多くのICカードシステムは、基本的に利用機が主、ICカードが従の関係にあり、ICカードは情報記憶媒体的な使われ方をされることがほとんどであったが、今後はICカード内に記憶されたアプリケーションプログラムが主体となってネットワーク上のサービスを受けるシステムが普及することが予想される。

【0008】例えば、ICカード内のアプリケーションプログラムが、ICカード内に格納されたアクセス情報から計算機ネットワーク上のどのリモートホストに、どのような手順でアクセスするかを判断し、同じくICカード内に格納されたデータ情報をリモートホストに送信する、もしくはリモートホストからデータ情報を取得してICカード内に格納する、といったシステムである。

【0009】より具体的な例として次のようなICカードシステムを考える。インターネットに代表される大規模計算機ネットワーク空間で、WWW(World Wide Web)に代表される仕組みを用いて多種のサービスが、それぞれ別個のリモートホスト(サーバサイト)によって運営されている。さらに、駅、店舗、公共施設等の、不特定多数の人間が訪れる場所に利用機を設置する。利用機の適例はキオスク端末である。キオスク端末は、不特定多数のユーザに情報提示や各種のサービスを行うことを目的とした計算機であり、ここではディスプレイ、プリンタ、タッチパネル、キーパッド等のユーザインタフェース、ネットワークインタフェース、ICカードリーダライタを持つものを想定する。

【0010】ユーザは、上記の利用機を用いてネットワーク上のサービスを利用するためのICカードを個々に所持し、行く先々に設置された任意の利用機にICカードを接続することで、それらのサービスを受けることができる。

【0011】サービスを受けるためのクライアントソフトウェアは、ICカード内にアプリケーションとして格

納される。即ち、どのようなアプリケーションをICカード内に持たせるかによって、ユーザが受けられるサービス内容が変わる。これはパーソナルコンピュータやワークステーションを用いてインターネット上のサービスを受ける場合と類似しており、原理的にはICカード内にWWWブラウザや電子メールクライアントを持たせることも可能である。

【0012】ICカード内にWWWブラウザを持たせた場合、ユーザはそのICカードを用いてインターネット上のウェブコンテンツ(WWWによって公開されるマルチメディア情報)を閲覧できる他、ウェブメール(WWWの仕組みを利用した個人向け電子メールサービス)、電子掲示板、オンラインショッピング等のサービスを受けられる。これにより、ユーザは携帯型コンピュータ等を持ち運ばなくとも、上記のICカードを1枚持ち歩くだけで、訪問先にある利用機からこれらのサービスを受けることが可能となる。これは、例えば携帯電話機のような小型通信情報機器を利用する場合と比較しても、画面解像度を始めとしたユーザインタフェースの品質、通信品質、ユーザ負担コスト等の面で優位性があるものと考えられる。

【0013】しかしながら、このようなICカードシステムを従来技術で実現しようとした場合、次のような問題が生じる。

【0014】第1に、ICカード内のアプリケーションによってユーザがアクセスしたネットワーク上のリモートホストの位置(インターネットであればホスト名、ドメイン名及びIPアドレス)が、利用機に掌握されてしまう。これは、ICカードそれ自体が利用機のICカードリーダライタとの間の低レベルな通信(一般的にはシリアル通信)機能しか持たず、ネットワーク通信の全てを利用機に依存していることに起因する。前記の従来例1~3に示される暗号応用技術によって、ICカードとリモートホストの間で交された通信内容は利用機に対し秘匿することが可能であるが、利用機からリモートホストへ直接ネットワーク通信のコネクションを張っている限り、アクセス先がどのホストであったのかを隠すことはできない。アクセス先が特定できると、そのユーザが受けたサービスの種類や性質を推定されることも有り得る(例:コンピュータゲームの通信販売サイトへアクセスしたユーザは、少なくともコンピュータゲームに興味があり、もしかしたらそのサイトで何か商品を購入した可能性もある、等)。ユーザのプライバシー保護の観点からはアクセス先情報の漏洩は好ましいことではない。

【0015】第2に、ICカード内のアプリケーションがユーザに提示した出力の内容、及びICカード内のアプリケーションに対してユーザが行った入力の内容が、全て利用機に掌握されてしまう。これは上記と同様、一般にICカードそれ自体がユーザインタフェースを持たず、全て利用機を介してユーザとのインタラクションを



行うことに起因する。具体的には、利用機の画面に表示あるいはプリンタにて印刷した出力内容は、それが文字であっても画像であっても、原理的に全て利用機がコピーを取得し、保存したり他に転用したりすることが可能である。また、ユーザからの入力についても同様であり、例えばアカウント情報やパスワード情報、クレジットカード番号等を利用機から直接入力した場合、それらの内容を利用機に対して秘匿することは不可能である。前記の従来例 1～5 に示した技術において、このような問題は考慮されていない。

【0016】ICカードのユーザが、利用機の運用者、運用ポリシー、悪意のある第三者に対するセキュリティ強度について充分納得し、利用機を信用できる場合には、上記のようなことは問題にならないが、そうでない場合 IC カードユーザは利用機を安心して使うことができない。

【0017】逆の見方をすると、従来は利用機を設置する場合、IC カードユーザ、及びリモートホスト運用者に対してセキュリティ上の保証をする必要があり、そのためにハードウェアの不正使用の防止対策、ネットワークからの不正行為対策に加え、運用母体と運用ポリシーを明確にし、設置した利用機が不正なもの、危険なものでないことを証明してオーソライズされる必要があった。これはハードウェア価格や運営コスト高騰の問題として顕在化する可能性が極めて高く、利用機普及の阻害要因となり、結果的に IC カードユーザが得るメリットも小さくなってしまふ。

【0018】本発明は上記のような問題点を解決するものであり、オーソライズ不要の安価なカード端末設置を可能とし、また IC カードユーザにとっては信頼度の低い、もしくは信頼度のはっきりしないカード端末装置を用いた場合でも、プライバシーや財産に関わる個人の機密情報を漏らすことなく、安全が保証できる範囲でのネットワーク利用が可能になる、セキュアかつ利便性の高い IC カードシステムを構築可能な IC カード装置及びプロキシ装置、並びにカード端末装置を提供することを目的とする。

【0019】

【課題を解決するための手段】上記の課題を解決するため本発明は、第 1 に、IC カード装置（IC カード）や通信相手先のリモートホストの代理として計算機ネットワーク上で代理装置などとして機能するプロキシ装置を設ける。プロキシ装置はネットワーク通信手段を持ち、カード端末装置（利用機）とリモートホストの両者と通信を行う。さらに、プロキシ装置にデータ変換手段を設け、IC カード装置からカード端末装置経由で受信したデータを、IC カード装置が既知かつカード端末装置が未知の変換アルゴリズムもしくはパラメータを用いてデータ変換を行う。IC カード装置には、送信用データ保持手段と、これに保持されているデータをカード端末装

置に送信するデータ送信手段とを設ける。カード端末装置には、IC カード装置からデータを受信するデータ受信手段と、データ受信手段が得たデータをプロキシ装置に送信するデータ転送手段とを設ける。これにより、IC カード装置がプロキシ装置に渡したデータは、IC カードユーザの意図通りに、かつカード端末装置のユーザにその内容を知られることなく、プロキシ装置内部において異なるデータに変化させることが可能となる。

【0020】第 2 に、上記の送信用データとして、IC カード装置内のアプリケーションがアクセスしようとするホストのネットワーク上の位置及び通信方法を得るための情報を準備する通信キーデータ生成手段を設ける。通信キーデータは、IC カード装置内のメモリに書かれたデータと同一のものをを用いても構わないし、IC カード装置内部で変換処理を行った結果を用いても構わない。ただし、通信キーデータそのものからカード端末装置が容易にアクセス先を特定できないこと、さらに、プロキシ装置は受け取った通信キーデータ及び予めプロキシ装置内部に持つプログラムとデータにより、アクセス先を特定できることの 2 点が条件となる。予め IC カード装置とプロキシ装置の二者で取り決めた、通信キーデータからアクセス先特定情報を得るための演算アルゴリズムと演算パラメータを利用することによりこの条件は満たされる。そして、プロキシ装置はアクセス先特定情報を用いてネットワーク上のリモートホストと通信を行う。これにより、IC カード装置はカード端末装置にアクセス先を知られることなく、リモートホストと通信を行うことが可能となる。

【0021】第 3 に、IC カード装置とプロキシ装置の二者間で暗号化に関するアルゴリズムと鍵情報を予め取り決め、この取り決めに基づいてカード端末装置に内容を知られることなく任意の情報をやりとりするための、セキュアパスを設ける。セキュアパスは IC カード装置とプロキシ装置間の両者が、この二者以外に情報を漏洩させることなく通信を行う、秘匿性を有する仮想的な通信経路である。これにより、IC カード装置とプロキシ装置は、中間に位置するカード端末装置に内容を知られることなく、任意の情報を片方向もしくは双方向にて送受可能となる。上記第 2 に示したアクセス先情報の引き渡しは、このセキュアパスを用いて行うことができる。その場合、IC カード装置内にてアクセス先情報を暗号化し（もしくは予め暗号化されたアクセス先情報を保持し）、この暗号化アクセス先情報をカード端末装置に引き渡し、カード端末装置はこれをそのままプロキシ装置に引き渡し、プロキシ装置は暗号化アクセス先情報を復号化して元のアクセス先情報を得る、という手順を踏むことにより行う。

【0022】暗号化及び復号化の方法は、IC カード装置とプロキシ装置の両者が予め保持する共通の鍵によって暗号化も復号化も行う対称鍵暗号方式、もしくは IC

カード装置が公開鍵で暗号化を行い、プロキシ装置が対となる秘密鍵で復号化を行う非対称鍵暗号方式などの従来技術を適用すれば良い。また、カード端末装置から引き渡された暗号化アクセス先情報がカード端末装置によって捏造されたものではないことをプロキシ装置が確認するために、同じく非対称鍵暗号方式を応用した従来技術である署名を暗号化アクセス先情報に付与することもできる。また、アクセス先情報に限らず、セキュアパスを用いてＩＣカード装置とプロキシ装置の二者間で任意のデータを秘密的にやりとりすることが可能である。

【００２３】第４に、上記セキュアパスを介してＩＣカード装置内におけるデータの暗号化手段を、アクセス先情報と、転送データ情報について個別に設ける。転送データ情報はプロキシ装置がさらにアクセス先のリモートホストに引き渡すデータ情報である。このとき、転送データの復号化については予めＩＣカード装置とリモートホストの二者間で取り決めておき、カード端末装置はもちろんプロキシ装置も転送データ復号用の鍵を持たないようにする。これにより、ＩＣカード装置がリモートホストに引き渡す転送データの内容を、カード端末装置だけでなくプロキシ装置にも隠蔽することが可能となる。同様に、リモートホストからＩＣカード装置に引き渡す転送データについても、ＩＣカードとリモートホストの二者間で取り決めた暗号化・復号化手段を用いることで、カード端末装置及びプロキシ装置に対して秘密性を有する通信が可能となる。

【００２４】第５に、ＩＣカード装置にはＵＩリクエスト情報送信手段を設け、プロキシ装置にＵＩリクエスト情報受信手段を設ける。ＵＩリクエスト情報はＩＣカード装置がどのようなユーザインタフェース（ＵＩ）をカード端末装置上に実現するかを示す情報であり、これはセキュアパスを介してＩＣカード装置からプロキシ装置に引き渡される。もしくは、ＵＩリクエスト情報そのものにセキュリティを求める必要がない場合は、暗号化しない生データの状態でＵＩリクエスト情報を送受しても良い。また、プロキシ装置にＵＩ情報送信手段を設け、カード端末装置にＵＩ情報受信手段とＵＩ実行手段を設ける。プロキシ装置はＩＣカードから受け取ったＵＩリクエスト情報に基づき、カード端末装置がＵＩを実現するのに必要な情報をＵＩ情報送信手段から発し、カード端末装置はＵＩ情報受信手段にてそれを受け取る。ＵＩ情報としては、ユーザに対する画面表示に用いる文字フォント、文字フォントからレンダリングした文字列画像データ等を用いる。これにより、ＩＣカード装置が想定するＵＩ実現に必要な文字フォントがカード端末装置上に存在しない場合でも、ＩＣカード装置の想定通りの文字列情報をカード端末装置の表示画面上もしくは印刷結果としてユーザに提示することが可能となる。

【００２５】第６に、上記第５に示すＵＩ情報として、カード端末装置上に予め設けられた動作環境に適合する

プログラム（実行手順と必要なデータを組にしたデータ列）を適用する。これにより、ＩＣカード装置が想定するＵＩが、カード端末装置に強く依存することなく独自のものとして実現可能となる。

【００２６】第７に、ＩＣカード装置とプロキシ装置のどちらか片方もしくは両方に、端末認証手段（利用機認証手段）と端末信頼度評価手段（利用機評価手段）を設ける。カード端末装置の認証は、予め定められた認証データもしくは定められた規則に基づく認証データ生成手段と、認証データをプロキシ装置もしくはＩＣカード装置に引き渡す認証データ送信手段をカード端末装置に設けることによって行う。プロキシ装置もしくはＩＣカード装置の端末認証手段は、カード端末装置の認証データ送信手段から受け取った認証データを読み取り、この認証データが予め定めた条件に合致するか否かを調べる。端末信頼度評価手段はこの認証結果を読み取り、条件に合致する場合はそのカード端末装置は信頼できる、合致しない場合は信頼できないとして信頼度の評価を行う。ここで、認証データの内容、生成方法、評価のための条件等は秘密のものとして扱い、信頼できないカード端末装置に漏洩しないようにする。また、認証データを複数種類とすることにより、評価結果をより細かく分類することも可能である。

【００２７】プロキシ装置がカード端末装置を認証、評価する場合は、ネットワーク上のアドレス情報等、偽証が困難なカード端末装置の固有情報を基に行うことができる。その際、ネットワークアドレス情報と信頼度を対応付ける表を参照する等の方法を用いることにより、カード端末装置の信頼度に複数の段階を設けることもできる。これらにより、ＩＣカード装置もしくはプロキシ装置が、カード端末装置の信頼度を獲得することができる。

【００２８】第８に、ＩＣカード装置とプロキシ装置の両方に、端末信頼度評価手段を設けてカード端末装置の信頼度情報を共有する。この場合、片方の端末信頼度評価手段が得たカード端末装置の評価結果を、セキュアパスを通じて他方に渡すようにする。これにより、ＩＣカード装置もしくはプロキシ装置のいずれか片方がカード端末装置の信頼度を獲得できた場合、もう一方にその情報を渡すことが可能となる。また、両方が個別にカード端末装置の信頼度を獲得した場合は、それぞれの評価結果を互いに確認し合うことが可能となる。

【００２９】第９に、ＩＣカード装置に送信情報制御手段を設ける。送信情報制御手段は、上記第７もしくは第８でＩＣカード装置が得たカード端末装置の信頼度評価結果を読み取り、信頼度に応じてＩＣカード装置からカード端末装置に送信する情報の内容に対して変更、削除、追加等の処理を行う。これにより、ＩＣカード装置からカード端末装置に送信する情報内容をカード端末装置の信頼度に従って異なるものにすることができる。ま

10

20

30

40

50

た、ICカード装置が機密情報として保持する情報をカード端末装置に送信しないよう上記送信情報制御手段を作用させる。機密情報の一つとして、ICカード装置が保持するユーザの個人情報などがある。これにより、信頼度の低いカード端末装置には個人情報を送らないなど、カード端末装置毎に異なるセキュリティレベルを用いた情報管理が可能となる。

【0030】第10に、プロキシ装置に送信情報制御手段を設ける。これは上記第9に示したICカード装置における送信情報制御手段と同様に、カード端末装置の信頼度評価結果に従ってプロキシ装置からカード端末装置に送信する情報の内容に対して変更、削除、追加等の処理を行う。また、ICカード装置と同様に、プロキシ装置が保持する機密情報をカード端末装置に送信しないよう上記送信情報制御手段を作用させる。これらにより、プロキシ装置からカード端末装置に送信する情報内容を、上記のICカード装置と同様にカード端末装置の信頼度に応じて異なるものにすることができ、信頼度の低いカード端末装置に機密情報を渡さないといったセキュリティ管理が可能となる。

【0031】第11に、プロキシ装置上において、上記第5に示したUI情報送信手段に、上記第10に示した送信情報制御手段を連動させ、カード端末装置の信頼度評価結果に従ってプロキシ装置からカード端末装置に送信するUI情報に対して変更、削除、追加等の処理を行うようにする。カード端末装置の信頼度が低いと端末信頼度評価手段が判断した場合、送信情報制御手段が作用して、プロキシ装置からカード端末装置に送信するUI情報のうち、ICカード装置が持つ機密情報をカード端末装置上の表示画面装置に出力してしまうようなUI部品を削除し、またICカードのユーザがカード端末装置の入力装置を通じて機密情報を入力してしまうようなUI部品を削除する。機密情報の一つとして、暗証番号、パスワード等がある。これらにより、信頼度の低いカード端末装置を使用する場合、機密情報をカード端末装置の画面上に表示し、それを取得されて漏洩してしまったり、また暗証番号等を不用意に入力して取得されてしまうようなトラブルの防止が可能となる。

【0032】第12に、ICカード装置もしくはプロキシ装置に、機密情報変換手段を設ける。上記のカード端末装置によるUI実行手段によって暗証番号、パスワード等の機密情報をユーザが直接入力する代わりに、機密情報を得るための第1の機密情報（仮の機密情報）を入力する。機密情報変換手段はこの第1の機密情報を読み取り、演算処理もしくは演算処理とデータ参照の組み合わせにより、第2の機密情報（真の機密情報）を生成する。機密情報変換手段をICカード装置が備える場合は、生成した真の機密情報をセキュアパスを通じてプロキシ装置に渡す。その後、プロキシ装置は、真の機密情報を用いてリモートホストと通信を行う。これにより、

カード端末装置のUIを通じて機密情報が漏洩する危険性を回避しつつ、機密情報を用いたネットワーク利用が可能となる。

【0033】機密情報変換手段が機密情報生成のための演算を行う際のデータの一つとして、ランダムなデータ（無作為に選択されたデータ）を用い、UI実行手段がこのランダムデータをユーザに提示し、提示されたランダムデータに従って異なる仮の機密情報をユーザに入力するよう促すことで、真の機密情報の生成アルゴリズム等を推測されにくくなり、より安全性を増すことが可能となる。さらに、誤って真の機密情報を入力しないようユーザに促す表示をUI実行手段が行うことで、ユーザの操作ミスによる機密情報漏洩を防止することが可能となる。

【0034】第13に、ICカード装置にプロキシ選択手段を設ける。プロキシ選択手段は、予め定めたルールに従ってネットワーク上に存在する複数のプロキシ装置候補から、使用するプロキシ装置を決定する。ルールとしては、ICカード装置が保持するプロキシ装置のリストから使用に適したプロキシ装置を逐次探す方法、ランダムで探す方法、またカード端末装置に問い合わせで最適候補を得る方法等がある。これらにより、ICカード装置毎、カード端末装置毎などの条件に従って異なるプロキシ装置が利用可能となり、ネットワーク負荷及びプロキシの処理負荷の集中が緩和できる。また、プロキシ情報操作手段をICカード装置に設ける。プロキシ情報操作手段は、ICカード装置のユーザがカード端末装置等を通じて個々のプロキシ装置へのアクセス方法と使用ルールなどのプロキシ情報を登録・変更・削除するものである。これによりICカード装置のユーザが使用するプロキシ装置を複数登録・変更することが可能となる。

【0035】第14に、ICカード装置にインセンティブ発行手段を設け、カード端末装置にインセンティブ獲得手段を設ける。インセンティブ発行手段はインセンティブ獲得手段との間で電子情報の授受を行うことにより、カード端末装置及びカード端末装置の所有者や運用者に対して金銭的、事業的なメリットを直接的もしくは間接的に与える。インセンティブの例として広告情報を考えた場合、カード端末装置はICカードユーザに対して商業広告等の情報を渡すことが可能となり、それが利用機運営のインセンティブとなる。また、インセンティブとして金銭もしくは何らかの有価物に関連した有価価値情報を授受することにより、カード端末装置は、ICカード装置から利用機使用の報酬としてより明確なインセンティブを得ることが可能となる。

【0036】上記第1から第14に関して、ICカード装置としては、ICカードに内蔵されるICチップと同等もしくは類似した機能構成をもつ他の装置においても適用できる。装置の例として、ICタグ、携帯電話機、携帯型情報端末、マイコン内蔵メモリカードなどが挙げ

られる。

【0037】また、上記第1から第14に関して、カード端末装置としては、不特定多数の人間が訪れる場所に設置する公共端末、不特定多数の人間が訪れる場所でレンタル品として貸し出される携帯電話機もしくは携帯型情報端末、不特定多数の人間にレンタル品として貸し出されるカーナビゲーション装置などを用いることができる。

【0038】また、上記第1から第14を構成する各装置を実現するためにコンピュータ上で動作するソフトウェアとして、磁気ディスク、光ディスク、半導体メディア等の情報記憶媒体に処理手順及びデータ等を格納しておき、コンピュータハードウェアがこれを読み取って所定の動作を行うようにしても、上記と同じ効果が得られる。

【0039】したがって、本発明にかかるICカードシステムにおいては、以下のような特徴的な構成を有する。

【0040】(1) 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うICカードシステム用のICカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段とを備え、前記カード端末装置と計算機ネットワークを介して接続されたリモートホストとデータ通信を行う際に、このリモートホストと前記カード端末装置との間に設けられるプロキシ装置と当該ICカード装置との間で予め定めたものであって、かつ、前記カード端末装置には未知のものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するためのデータを前記プロキシ装置へ送信するもの。

【0041】(2) 前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を、前記カード端末装置が解釈困難なキーデータとして生成する通信キーデータ生成手段を備え、前記変換アルゴリズムもしくは変換パラメータとして、当該ICカード装置と前記プロキシ装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いてデータ変換処理を実行する際に、前記通信キーデータを前記プロキシ装置へ送信するもの。

【0042】(3) 通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記プロキシ装置または前記リモートホストとの間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成するもの。

(4) 前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記プロキシ装置との間で形成したセキュアパスを経由して該プロキシ装置へ送るもの。

【0043】(5) 前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順を異なる鍵情報を用いることによりデータの暗号化を行う第2の暗号処理手段を備え、前記第2の暗号処理手段により当該ICカード装置が保持する任意のデータを暗号化し、この第2の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第2の暗号化データを前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送るもの。

【0044】(6) 前記リモートホストのアクセス先情報の暗号化とは異なる暗号化手順もしくは同一の暗号化手順を異なる鍵情報を用いることによりデータの暗号化を行う第2の暗号処理手段を備え、前記第2の暗号処理手段により当該ICカード装置が保持する任意のデータを暗号化し、この第2の暗号化データは前記プロキシ装置において復号不能で前記リモートホストにおいて復号可能となっており、前記第2の暗号化データを前記リモートホストのアクセス先情報の暗号化データと共に前記リモートホストとの間で形成したセキュアパスを経由して前記プロキシ装置へ送るもの。

【0045】(7) 当該ICカード装置と前記プロキシ装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成するもの。

(8) 当該ICカード装置と前記プロキシ装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパスを形成するもの。

【0046】(9) 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うICカードシステム用のICカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置において実現するユーザインタフェースに関わるUIリクエスト情報を、このカード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置に送信するUIリクエスト情報送信手段とを備えたもの。

【0047】(10) 前記UIリクエスト情報として、文字コードに関わる文字列情報を用いるもの。

(11) 前記UIリクエスト情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させるためのプログラム情報による動作結果に影響を与えるパラメータ情報を用いるもの。

【0048】(12) 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行うICカードシステム用のICカード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置の認証を行

う端末認証手段と、前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記カード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記プロキシ装置へ送るもの。

【0049】(13) 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行う IC カードシステム用の IC カード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記カード端末装置が接続された計算機ネットワーク上において設けられるプロキシ装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記プロキシ装置から前記カード端末装置の信頼度評価結果を受け取るもの。

【0050】(14) 前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えるもの。

(15) 前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対して IC カード装置から送信する情報の一部もしくは全てを削除もしくは変更するもの。

【0051】(16) 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該 IC カード装置が保持する機密情報に関わる情報を削除もしくは変更するもの。

(17) 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該 IC カード装置が保持する IC カードユーザのプライバシーに関わる情報を削除もしくは変更するもの。

【0052】(18) 半導体記憶手段を有してなり、カード端末装置とデータのやり取りを行う IC カードシステム用の IC カード装置であって、送信用のデータを保持する送信用データ保持手段と、前記送信用データ保持手段からデータを読み出して前記カード端末装置へ送信するデータ送信手段と、前記カード端末装置と計算機ネットワークを介して接続されたリモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報変換手段とを備え、前記機密情

報変換手段は前記カード端末装置より入力された第 1 の機密情報データを当該カード端末装置に対して秘匿性を持った第 2 の機密情報データに変換し、この第 2 の機密情報データを前記カード端末装置と前記リモートホストとの間に設けられるプロキシ装置へ送るもの。

【0053】(19) 前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じて IC カードユーザに提示し、前記カード端末装置より入力された第 1 の機密情報データから前記変換キーデータを用いて前記第 2 の機密情報データを生成するもの。

(20) 前記変換キーデータと前記第 1 の機密情報データとを一对一に対応させて同一の第 2 の機密情報データを生成するための異なるデータの組を複数設けたもの。

【0054】(21) 前記カード端末装置において実現するユーザインタフェースに関わる UI リクエスト情報を前記プロキシ装置に送信する UI リクエスト情報送信手段を備え、前記 UI リクエスト情報として、前記リモートホストから要求される機密情報として前記第 2 の機密情報データの代わりに前記第 1 の機密情報データを入力すべきことを IC カードユーザに指示するための UI 部品情報を用いるもの。

【0055】(22) 予め定めた規則に従って計算機ネットワーク上の複数のプロキシ装置の中から一つを選択するプロキシ選択手段を備えたもの。

(23) 前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置を逐次的に検索して選択するもの。

(24) 前記プロキシ選択手段は、予め登録されたプロキシ装置のリストから使用に適するプロキシ装置をランダムに検索して選択するもの。

(25) 前記プロキシ選択手段は、前記カード端末装置に問い合わせ使用に適するプロキシ装置を選択するもの。

(26) 使用に適するプロキシ装置を選択するためのプロキシ装置のリストを有し、このリスト内容の追加、変更、削除の少なくともいずれか一つを行うプロキシ情報操作手段を備えたもの。

【0056】(27) 前記カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態を電子情報のやりとりによって生じさせるインセンティブを発行するインセンティブ発行手段を備え、このインセンティブに関する情報を前記カード端末装置との間で通信するもの。

(28) 前記インセンティブとして広告情報を用い、前記インセンティブ発行手段は前記カード端末装置からこの広告情報を受信するもの。

(29) 前記インセンティブとして金銭あるいは有価価値物に関連した有価価値電子情報を用い、前記インセンティブ発行手段はこの有価価値電子情報を前記カード端末装置

に送信するもの。

【0057】(30) ICカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる ICカードシステム用のプロキシ装置であって、前記 ICカード装置と当該プロキシ装置との間で予め定めたものである変換アルゴリズムもしくは変換パラメータを用いてデータ変換処理を実行するデータ変換手段を備えたもの。

【0058】(31) 前記データ変換手段は、前記リモートホストと通信を行う際に必要となるアクセス先を特定するためのアクセス先情報を前記カード端末装置が解釈困難なキーデータとして生成した通信キーデータを変換するもので、前記変換アルゴリズムもしくは変換パラメータとして、当該プロキシ装置と前記 ICカード装置の二者間で予め取り決めたものであって、かつ、前記カード端末装置において未知の演算アルゴリズムもしくは演算パラメータを用いて変換処理を行うもの。

【0059】(32) 通信するデータの暗号化と復号化の少なくとも一方を行う暗号処理手段を備え、前記 ICカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成するもの。

(33) 前記暗号処理手段によって前記リモートホストのアクセス先情報を暗号化し、この暗号化データを前記 ICカード装置との間で形成したセキュアパスを経由して該 ICカード装置から受け取るもの。

【0060】(34) 当該プロキシ装置と前記 ICカード装置が同一の鍵情報を用いて暗号化及び復号化を行う対称鍵暗号方式を用いてセキュアパスを形成するもの。

(35) 当該プロキシ装置と前記 ICカード装置が互いに関連をもつ非同一の鍵情報を用いて暗号化及び復号化を行う非対称鍵暗号方式を用いてセキュアパスを形成するもの。

【0061】(36) ICカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる ICカードシステム用のプロキシ装置であって、前記カード端末装置において実現するユーザインタフェースに関わる UI リクエスト情報を受信する UI リクエスト情報受信手段と、前記受信した UI リクエスト情報の内容に基づいて前記カード端末装置におけるユーザインタフェース部品に関わる UI 情報を前記カード端末装置に送信する UI 情報送信手段とを備えたもの。

【0062】(37) 前記 UI 情報として、文字フォントに関わる文字画像情報を用いるもの。

(38) 前記 UI 情報として、前記カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用い

るもの。

(39) 前記 UI 情報として、前記カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いるもの。

【0063】(40) ICカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる ICカードシステム用のプロキシ装置であって、前記カード端末装置の認証を行う端末認証手段と、前記認証結果を基に前記カード端末装置の信頼度を評価する端末信頼度評価手段と、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記 ICカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記カード端末装置の信頼度評価結果を前記 ICカード装置へ送るもの。

【0064】(41) ICカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられる ICカードシステム用のプロキシ装置であって、データの暗号化と復号化の少なくとも一方を行う暗号処理手段とを備え、前記 ICカード装置との間で暗号化されたデータを受け渡すための秘匿性を持った通信路であるセキュアパスを形成し、このセキュアパスを介して前記 ICカード装置から前記カード端末装置の信頼度評価結果を受け取るもの。

(42) 前記端末認証手段と前記端末信頼度評価手段の少なくとも一方が、前記カード端末装置の計算機ネットワークへの接続に関わる固有かつ一意の情報を用いて動作するもの。

【0065】(43) 前記カード端末装置に送信する任意のデータについて送信前に情報内容の制御処理を行う送信情報制御手段を備え、この送信情報制御手段は、前記カード端末装置の信頼度評価結果に基づいて前記カード端末装置へ送る情報の一部もしくは全部に対して変更を加えるもの。

(44) 前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対してプロキシ装置から送信する情報の一部もしくは全てを削除もしくは変更するもの。

(45) 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持する機密情報に関わる情報を削除もしくは変更するもの。

(46) 前記送信情報制御手段は、前記カード端末装置に送信する情報のうち、当該プロキシ装置が保持する ICカードユーザまたはプロキシユーザのプライバシーに関わる情報を削除もしくは変更するもの。

【0066】(47) 前記カード端末装置において実現するユーザインタフェース部品に関わる UI 情報を前記

10

20

30

40

50

カード端末装置に送信するUI情報送信手段を備え、前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対してプロキシ装置からUI情報を送信する前に、前記UI情報の中から機密情報表示に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後のUI情報を前記カード端末装置へ送るもの。

【0067】(48) 前記カード端末装置において実現するユーザインタフェース部品に関わるUI情報を前記カード端末装置に送信するUI情報送信手段を備え、前記送信情報制御手段は、前記信頼度評価結果としてカード端末装置の信頼度が低く送信した情報が不正に利用される可能性があるとして認識された場合に、当該カード端末装置に対してプロキシ装置からUI情報を送信する前に、前記UI情報の中から機密情報入力に関わる部分を削除もしくは機密を保護する状態に変更し、その処理後のUI情報を前記カード端末装置へ送るもの。

【0068】(49) ICカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられるICカードシステム用のプロキシ装置であって、前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報の変換を行う機密情報変換手段を備え、前記機密情報変換手段は前記カード端末装置より入力された第1の機密情報データを当該カード端末装置に対して秘匿性を持った第2の機密情報データに変換し、この第2の機密情報データを前記リモートホストへ送るもの。

【0069】(50) ICカード装置とデータのやり取りを行うカード端末装置とこれに計算機ネットワークを介して接続されたりリモートホストとの間に設けられるICカードシステム用のプロキシ装置であって、前記リモートホストからの要求に応じて前記カード端末装置を用いて入力する機密情報に関して、前記カード端末装置より入力された第1の機密情報データが当該カード端末装置に対して秘匿性を持った状態に変換された第2の機密情報データを、前記ICカード装置から受け取って前記リモートホストへ送る機密情報獲得手段を備えたもの。

【0070】(51) 前記機密情報変換手段は変換用の変換キーデータを生成してこれを前記カード端末装置を通じてICカードユーザに提示し、前記カード端末装置より入力された第1の機密情報データから前記変換キーデータを用いて前記第2の機密情報データを生成するもの。

(52) 前記変換キーデータと前記第1の機密情報データとを一对一に対応させて同一の第2の機密情報データを生成するための異なるデータの組を複数設けたもの。

【0071】(53) 前記カード端末装置において実現するユーザインタフェース部品に関わるUI情報を前記

カード端末装置に送信するUI情報送信手段を備え、前記UI情報として、前記リモートホストから要求される機密情報として前記第2の機密情報データの代わりに前記第1の機密情報データを入力すべきことをICカードユーザに指示するためのUI部品情報を用いるもの。

【0072】(54) ICカード装置とデータのやり取りを行うICカードシステム用のカード端末装置であって、当該カード端末装置は計算機ネットワーク上に於て設けられるプロキシ装置と接続され、前記プロキシ装置から送られた当該カード端末装置におけるユーザインタフェース部品に関わるUI情報を受信するUI情報受信手段と、前記受信したUI情報の内容に基づいて前記ICカード装置とのデータ通信に関するユーザインタフェースを実行するUI実行手段とを備えたもの。

【0073】(55) 前記UI情報として、文字フォントに関わる文字画像情報を用いるもの。

(56) 前記UI情報として、当該カード端末装置のユーザインタフェースに関わるハードウェアを動作させる手順及びデータのまとまりであるプログラム情報を用いるもの。

(57) 前記UI情報として、当該カード端末装置の種類または構成もしくは動作状態によって異なるプログラム情報を用いるもの。

【0074】(58) ICカード装置とデータのやり取りを行うICカードシステム用のカード端末装置であって、当該カード端末装置は計算機ネットワーク上に於て設けられる複数のプロキシ装置と接続され、前記ICカード装置からの問い合わせに応じて、予め定めた規則に従って使用に適するプロキシ装置を選択するための処理を行うプロキシ選択処理手段を備えたもの。

【0075】(59) 当該カード端末装置の所有者もしくは運用者に対して金銭的もしくは事業的に有利となる状態を電子情報のやりとりによって生じさせるインセンティブを受けるインセンティブ獲得手段を備え、このインセンティブに関する情報を前記ICカード装置との間で通信するもの。

(60) 前記インセンティブとして広告情報を用い、前記インセンティブ獲得手段はこの広告情報を前記ICカード装置に送信するもの。

(61) 前記インセンティブとして金銭あるいは有価価値物に関連した有価電子情報を用い、前記インセンティブ獲得手段は前記ICカード装置からこの有価電子情報を受信するもの。

【0076】(62) 上記(1)～(29)のいずれかに記載のICカードシステム用のICカード装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

(63) 上記(30)～(53)のいずれかに記載のICカードシステム用のプロキシ装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情



報記録媒体。

(64) 上記(54)～(61)のいずれかに記載のICカードシステム用のカード端末装置を実現するための処理手順及びデータを記録したコンピュータ読取可能な情報記録媒体。

【0077】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

【0078】 [第1実施形態] 図1は本発明の第1実施形態に係るICカードシステムの構成を示すブロック図である。

【0079】 本実施形態のICカードシステムは、半導体記憶手段を搭載したカード本体を含むICカード装置に相当するICカード101、ICカード101とデータ通信を行うカード端末装置に相当する利用機102、ICカード101に対して情報の提供等を行うホストコンピュータであるリモートホスト104、利用機102とリモートホスト104との間に設けられICカード101とリモートホスト104の両者に対してデータ通信を行うプロキシ装置103を備えて構成される。利用機102とプロキシ装置103の間、及びプロキシ装置103とリモートホスト104の間は、インターネット等の計算機ネットワーク105によって接続されている。なお、利用機102とリモートホスト104は、共通の計算機ネットワークに接続されていても、また異なる計算機ネットワークに接続されていても良いが、プロキシ装置103は、利用機102及びリモートホスト104の両者とそれぞれ共通の計算機ネットワークに接続され、両者と通信が可能なように構成されている。

【0080】 利用機102にはICカードリーダライタ108が設けられている。ICカード101として接触型ICカードを適用した場合、ICカード101はICカードリーダライタ108に挿入もしくは接続され、電気信号を用いて利用機102と通信を行う。また、ICカード101に非接触型ICカードを適用した場合には、ICカード101はICカードリーダライタ108との間で電波信号をやりとりすることにより、利用機102と通信を行う。

【0081】 ICカード101は、内部に送信用データ保持手段106とデータ送信手段107とを備えている。送信用データ保持手段106は、ICカード101に内蔵されるICチップのメモリ等を用いて実現される。データ送信手段107は、送信用データ保持手段106が保持するデータを読み取ってICカードリーダライタ108に送信するもので、ICカード101に内蔵される通信ハードウェア及びそれを駆動するための処理装置とソフトウェアプログラムによって実現される。

【0082】 なお、以下の実施形態において示す機能的構成による各手段は、前記データ送信手段107と同様に、各構成装置がもつハードウェアと、それを駆動する

ための処理装置及びソフトウェアプログラムにより実現されるものである。

【0083】 利用機102は、内部にICカードリーダライタ108からデータを受け取るデータ受信手段109と、データ受信手段109が受信したデータを計算機ネットワーク105を介してプロキシ装置103に送信するデータ転送手段110とを備えている。

【0084】 プロキシ装置103は、内部に計算機ネットワーク105を介して利用機102から受信したデータを別のデータに変換するデータ変換手段111を備えている。このプロキシ装置103は、データ変換手段111が作成した変換後のデータを、計算機ネットワーク105を介してリモートホスト104に送信し、リモートホスト104はこれを受信する。

【0085】 ICカード101が利用機102を介してプロキシ装置103と通信を開始するに先立って、予めICカード101内のアプリケーションプログラムとプロキシ装置103のデータ変換手段111との間で、データ変換の規則と方法についての取り決めを作っておく。

【0086】 例えば、 $x$ というデータを与えた場合は $f(x)$ というデータに変換される規則とし、変換方法 $f$ についてICカード101とプロキシ装置103のみが知っている状態を作る。この取り決めはICカード101の発行以前に行っても良いし、ICカード101の発行後も、ICカード101とプロキシ装置103との間で十分にセキュアな通信が可能な条件下であれば行うことができる。

【0087】 ICカード101のユーザがリモートホスト104にデータを送信する場合、ICカード101の送信用データ保持手段106にデータ $x$ を格納し、データ送信手段107はこのデータ $x$ を利用機102のICカードリーダライタ108を介してデータ受信手段109に送る。次に、データ受信手段109はデータ転送手段110にデータ $x$ を渡し、データ転送手段110はデータ $x$ を計算機ネットワーク105を介してプロキシ装置103のデータ変換手段111に送る。

【0088】 ここで、利用機102は変換方法 $f$ を知らないため、プロキシ装置103の内部でデータ変換手段111が出力するデータ $f(x)$ を知ることはできない。よって、プロキシ装置103が $f(x)$ を用いてリモートホスト104と通信を行えば、結果としてICカード101のユーザは利用機102に知られることなくデータ $f(x)$ を用いた通信をリモートホスト104との間で行うことが可能となる。

【0089】 特に、 $f(x)$ を逆変換可能なものに定め、 $f$ の逆変換を $g(y)$ としたとき、ICカード101は $g(y)$ を送信用データ保持手段106に置くことにより、データ $y$ を利用機102に知られることなくリモートホスト104に送ることが可能となる。その際、



リモートホスト 104 には  $f(x)$  を得るためのデータ変換手段は不要である。さらに、プロキシ装置 103 はそれ自身がネットワークを利用してリモートホスト 104 と通信を行えるため、従来は利用機 102 に依存していたネットワーク通信、ユーザインタフェース形成等に関わる情報を全て利用機 102 に秘匿しつつ、プロキシ装置 103 が得ることが可能となる。

【0090】上記のようなプロキシ装置は不正侵入が困難な安全な建物内等に設置することが容易であり、これは街頭等の不特定多数の人間が出入りする場所に置かれる利用機と比較してセキュリティ強度を容易に高めることが可能である。通常、キオスク端末用として専用に作られた計算機は特に強固なセキュリティを確保したハードウェアを使用するが、本実施形態によれば、そのようなハードウェアを使用しなくとも IC カードユーザに被害を及ぼし難い利用機を設置できる。また、IC カードユーザもセキュリティ強度の弱い利用機を安全に利用できることになり、その実用的効果は大きい。

【0091】このように、本実施形態の構成では、IC カードユーザは利用機に通信内容を知られることなく IC カードとプロキシ装置との間で通信を行うことができるため、アクセス先や通信内容を秘匿してセキュリティを確保した状態で利用機を使用することが可能となる。よって、利用機において必ずしも強固なセキュリティ上の保証をする必要がなく、利用機設置に関するハードウェア価格や運営コストを低減することも可能である。IC カードユーザは、街頭等の不特定多数の人間が訪れる場所に設置している場合など、利用機の信頼度が不明確な場合であっても十分なセキュリティを確保でき、安心して使用することができる。

【0092】〔第 2 実施形態〕図 2 は本発明の第 2 実施形態に係る IC カードシステムの構成を示すブロック図である。第 2 実施形態は、第 1 実施形態と同様に、インターネット上のサービスを受けるアプリケーションを搭載した IC カード 201、リモートホスト 204 を備えて構成される。これらは、図 2 で模式的に示すインターネット空間 205 に設けられる。利用機 202 とプロキシ装置 203、及びプロキシ装置 203 とリモートホスト 204 は、それぞれインターネット空間 205 において形成されるネットワークコネクション（仮想的なデータ通信経路を持つ関係）206、207 により接続される。なお、個々の装置が具備する手段は図 1 の第 1 実施形態と同様である。

【0093】IC カード 201 に載せるアプリケーションとしては、インターネット上のリモートホスト 204（World Wide Web サービスを提供するウェブサイト）へアクセスし、リモートホスト 204 からの情報を IC カード 201 内のメモリに取得、もしくは IC カード 201 内のメモリに保持している情報をリモートホスト 204 に登録するソフトウェアを想定する。

【0094】図 3 は、本実施形態におけるアクセス先情報及び通信キーデータの関係を例示したものである。ここで、符号 301 は IC カード 201 のアプリケーションがアクセスしようとするリモートホスト 204 のインターネットにおける存在場所（URL）を記したアクセス先情報であり、符号 302 はアクセス先情報 301 から第 1 実施形態に示した変換  $g$  によって得た通信キーデータである。なお、アクセス先情報 301 と変換  $g$  は省略し、初めから変換済みの通信キーデータ 302 を保持していても良い。また、符号 303 及び 304 は通信キーデータ 302 がそれぞれ利用機 202 とプロキシ装置 203 に渡った状態を示すもので、通信キーデータ 302 と同一のものである。符号 305 は通信キーデータ 304 から変換  $f$  によって得られるアクセス先情報であり、アクセス先情報 301 と同一のものとなる。

【0095】図 4 は本実施形態におけるアクセス先秘匿処理の流れを示したフローチャートであり、図 1～3 と合わせて以下その動作を説明する。IC カード 201 のユーザは、IC カード 201 を利用機 202 に挿入することにより上記のインターネットサービスを受けられる。ここで利用機 202 は、例えば街頭、駅、公共施設、店舗等に置かれた共用端末で、不特定多数のユーザが利用することを前提に設置され、IC カード 201 のユーザは利用機 202 の運用、管理のポリシー等について知らされていない状況を想定する。

【0096】IC カード 201 は、まずアクセス先の URL（Uniform Resource Locator；サービス提供ホストのインターネット空間におけるホスト特定情報（ドメイン名及びサーバ名など）と基本的な通信プロトコルとを含んだ文字情報）を示すアクセス先情報 301 を  $g$  で変換し（ステップ 401）、通信キーデータ 302 を生成して送信データ保持手段 106 に格納する（ステップ 402）。次いで、データ送信手段 107 を用いて通信キーデータ 302 を IC カードリーダライタ 108 を介して利用機 202 に送信する（ステップ 403）。

【0097】次に、利用機 202 はデータ受信手段 109 を用いて通信キーデータ 303 を受信する。（ステップ 404）。続いて、利用機 202 はプロキシ装置 203 と通信するためのネットワークコネクション 206 をインターネット空間 205 内に形成する（ステップ 405）。なお、コネクション形成の際に用いるプロキシ装置 202 の URL は、利用機 202 が予め保持していても良いし、既知の IC カード・利用機間通信技術を用いて IC カード 201 から利用機 202 に伝達しても良い。

【0098】ネットワークコネクション 206 を形成した後、利用機 202 はデータ転送手段 110 を用いて通信キーデータ 303 を内容を改変せずにプロキシ装置 203 に送信し（ステップ 406）、プロキシ装置 203 はこれを通信キーデータ 304 として受信する（ステッ

プ407)。利用機202が通信キーデータ303を改変せずに転送したことは、既知のデータ照合技術を用いて確認できる。

【0099】次に、プロキシ装置203はデータ変換手段111を用いて通信キーデータ304に対し変換fを行い(ステップ408)、ICカード201が意図した通りのアクセス先情報305を獲得する(ステップ409)。最後に、プロキシ装置203は獲得したアクセス先情報305から得たリモートホスト204の情報(URL等)を用いて、インターネット空間205内にネットワークコネクション207を形成する(ステップ410)。

【0100】なお、本実施形態ではアクセス先情報301及び305をURLとした構成例を示したが、その他のホスト特定情報及び通信方法特定情報によって構成することもできる。また、本実施形態では計算機ネットワークとしてインターネットを適用した構成例を示したが、無線ネットワークを含めたその他の計算機ネットワークによって構成することもできる。

【0101】また、本実施形態に示した処理フローに先立ち、従来の認証技術を用いてICカード201とプロキシ装置203の両者間で認証を行うことにより、利用機202とプロキシ装置203が示し合わせてICカード201を騙すことによる不正行為を防止することができる。この不正行為の例としては、プロキシ装置203が獲得したアクセス先情報305を、プロキシ装置203自身が利用機202に教えてしまうことが考えられる。なお、このような不正行為を防止するために、ICカード201はプロキシ装置203に情報を渡す処理に先立ち、プロキシ装置203が正当でかつ安全であることを確認すべきである。これは本発明における他の実施形態においても同様である。

【0102】以上のように、ICカードが発する通信キーデータを図3のようにプロキシ装置がアクセス先情報に変換することによって、利用機がリモートホストに対して直接ネットワークコネクションを形成することなくなるため、ICカード上のアプリケーションが計算機ネットワーク上のどのホストに、どのような方法でアクセスしたかの情報が利用機を通じて漏洩する問題が回避され、その実用的効果は大きい。この本実施形態の手段によって、[発明が解決しようとする課題]の欄に示した第1の問題点を明確に解決することができる。

【0103】[第3実施形態]図5は本発明の第3実施形態に係るICカードシステムの構成を示すブロック図である。第3実施形態は、第1実施形態と同様に、ICカード501、利用機502、プロキシ装置503、リモートホスト504を有して構成され、利用機502とプロキシ装置503、及びプロキシ装置503とリモートホスト504はそれぞれ計算機ネットワーク505を介して接続される。利用機502はICカードリーダ

イタ506を具備している。これらは図1の第1実施形態における各装置と同様な構成要素を持っている。

【0104】ICカード501は、内部に既知の暗号技術を用いて情報の暗号化及び復号化を行う暗号処理手段507を備えている。プロキシ装置503は、内部に暗号処理手段507と対になって一方が暗号化した情報を他方が復号化する暗号処理手段の機能を併せ持ったデータ変換手段508を備えている。これらの暗号処理手段507とデータ変換手段(暗号処理手段)508との間には、セキュアパス509が形成される。

【0105】このセキュアパス509は、ICカード501の暗号処理手段507が暗号化したデータを第1実施形態と同様の方法でプロキシ装置503のデータ変換手段508に渡すことによって、利用機502に内容を秘匿しながら情報を伝達することにより形成されるセキュアな(所望のセキュリティを確保した)仮想的データ通信経路である。また、プロキシ装置503のデータ変換手段508が情報の暗号化を行い、第1実施形態と逆方向にデータを送信し、さらにICカード501の暗号処理手段507が情報を復号化することにより、セキュアパス509は双方向のデータ通信経路となる。プロキシ装置503は、セキュアパス509を通じてICカード501から得た情報を用いてリモートホスト504と通信を行い、またリモートホスト504から得た情報をセキュアパス509を通じてICカード501に渡す。

【0106】以上のように、本実施形態ではICカード501とプロキシ装置502の間にセキュアパス509を設けることにより、利用機502に内容を秘匿しながらICカード501とリモートホスト504との間の通信が可能となる。その際、リモートホスト504にはICカード501の暗号処理手段507と対になる暗号処理手段を付加する必要がない。このため、リモートホスト504として既存のインターネットサービスホストを適用した場合、ホストの構成を変更せずにICカード501との間でセキュアなデータ送受が可能となる。

【0107】また、サービスの性格によってプロキシ装置503とリモートホスト504の間で独自のセキュリティ処理を施すことも容易であり、あるいはプロキシ装置503とリモートホスト504の間ではセキュリティ手段を設けず、課金等に関するセキュアな処理は全てプロキシ装置503が行うというような適用も可能であり、その実用的効果は大きい。

【0108】[第4実施形態]第4実施形態として、図2に示したICカードシステムの構成、図3に示したデータフロー及び図4に示した処理フローと同様の処理を、図5に示したセキュアパスを用いて実現したシステムも例示できる。すなわち、ICカード201が保持するアクセス先情報301を、暗号処理手段507を用いて暗号化し、セキュアパス509を通じてプロキシ装置203のデータ変換手段508に渡し、アクセス先情報

305を得るものである。

【0109】この実施形態では、第2実施形態と同等の効果が得られるが、さらにセキュアパスを使うことにより、アクセス先のみでなくネットワークコネクション形成後の通信内容も全て利用機に対して秘匿できる効果がある。第4実施形態によって、第2実施形態と同様に

【発明が解決しようとする課題】の欄に示した第1の問題点を明確に解決することができる。

【0110】【第5実施形態】図6は本発明の第5実施形態に係るICカードシステムの構成を示すブロック図である。第5実施形態は、第1実施形態と同様に、ICカード601、利用機602、プロキシ装置603、リモートホスト604を有して構成され、利用機602とプロキシ装置603、及びプロキシ装置603とリモートホスト604はそれぞれ計算機ネットワーク605を介して接続される。利用機602はICカードリーダライタ606を具備している。これら各構成装置の基本的な構成と関係は図1の第1実施形態と同様である。

【0111】ICカード601は、内部に既知の暗号技術を用いて情報の暗号化及び復号化を行う第1の暗号処理手段607及び第2の暗号化手段610を備えている。第1の暗号処理手段607と第2の暗号化手段610とは、互いに異なる暗号処理の仕組みを用いるか、もしくは同一の暗号処理の仕組みを異なる鍵を用いて利用する構成をとる。プロキシ装置603は、内部に第1の暗号化手段607と対になってセキュアパス609を形成する第1の復号化手段608を備えている。また、リモートホスト604は、内部に第2の暗号化手段610と対になってセキュアパス612を形成する第2の復号化手段611を備えている。

【0112】この場合、初めは第2の暗号化手段610が生成した暗号化データはセキュアパス609を介してプロキシ装置603に渡す。もしくは、利用機602による復号が困難であるという条件を満足すれば、セキュアパス609を介さずにプロキシ装置603に渡しても良い。いずれの場合もプロキシ装置603は第2の暗号化手段610が生成したデータをそのままリモートホスト604に転送する。これにより、ICカード601とリモートホスト604を直接結ぶ新たなセキュアパス612が形成される。

【0113】なお、本実施形態では各暗号化手段と各復号化手段の働きで各セキュアパスを単方向の通信に用いる例で説明したが、暗号化と復号化を逆に用いる構成を採ることにより、各セキュアパスを双方向通信に用いることも可能である。

【0114】上記のように、本実施形態によれば、ICカード601のユーザ及びICカード601内に設けたアプリケーションは、セキュアパス609を用いて利用機602に情報を秘匿しながらプロキシ装置603とセキュアな通信を行うことができ、さらにセキュアパス6

12を用いて利用機602に情報を秘匿しながらリモートホスト611とセキュアな通信を行うことができる。さらに、各暗号化手段及び復号化手段の暗号強度を十分に確保すれば、利用機及びプロキシ装置以外にも、データ通信経路上の様々な装置もしくは手段による情報の漏洩を防ぐことが可能となり、その実用的効果は大きい。

【0115】【第6実施形態】第6実施形態として、図6の構成において、ICカード601からプロキシ装置603へ、セキュアパス609を用いてリモートホスト604のアクセス先情報を渡し、さらにICカード601からリモートホスト604へ、セキュアパス612を用いてアクセス先情報以外の任意の情報を渡すようなシステムも例示できる。この場合、第5実施形態の効果に加えて、ICカード601とリモートホスト604の間において、利用機602だけでなくプロキシ装置603に対しても情報を秘匿した通信を可能にする効果がある。

【0116】【第7実施形態】第7実施形態として、図5における暗号処理手段507、データ変換手段508、あるいは図6における第1の暗号化手段607、第1の復号化手段608、第2の暗号化手段610、第2の復号化手段611を、それぞれ相互に対応関係を持つ手段間において共通の鍵を用いる対称鍵暗号方式を用いて実現したシステムも例示できる。この実施形態によれば、第3～第6実施形態と同等の効果が得られる。

【0117】【第8実施形態】第8実施形態として、図5における暗号処理手段507、データ変換手段508、あるいは図6における第1の暗号化手段607、第1の復号化手段608、第2の暗号化手段610、第2の復号化手段611を、それぞれ相互に対応関係を持つ手段間において互いに対応付けられた異なる鍵を用いる非対称鍵暗号方式を用いて実現したシステムも例示できる。非対称暗号方式としては既知の公開鍵暗号方式が適用できる。

【0118】また、第7実施形態に示した構成と組み合わせ、非対称暗号によって対称鍵暗号を渡し、セキュアパスを流れる情報の一部を対称鍵暗号を用いて秘匿化することもできる。この場合、第3～第6実施形態と同等の効果が得られる他、鍵交換の簡便性と暗号処理の高速性を得ることができる効果がある。

【0119】【第9実施形態】図7は本発明の第9実施形態に係るICカードシステムの構成を示すブロック図である。第9実施形態は、第1実施形態と同様に、ICカード701、利用機702、プロキシ装置703、リモートホスト704を有して構成され、利用機702とプロキシ装置703、及びプロキシ装置703とリモートホスト704はそれぞれ計算機ネットワーク705を介して接続される。利用機702はICカードリーダライタ706を具備している。これら各構成装置の基本的な構成と関係は図1の第1実施形態と同様である。

【0120】ICカード701は、ICカード701のユーザもしくはアプリケーションが求めるユーザインタフェース（以下、適宜UIと略記する）に関わる情報（以下、UIリクエスト情報と記する）を送信するUIリクエスト情報送信手段707を備えている。プロキシ装置703は、前記UIリクエスト情報を受けるUIリクエスト情報受信手段708と、利用機702におけるユーザインタフェースの形成と動作に関わる情報（以下、UI情報と記する）を送信するUI情報送信手段709とを備えている。また、利用機702は、前記UI情報を受けるUI情報受信手段710と、ユーザインタフェースの形成及び動作の処理を行うUI実行手段711とを備えている。

【0121】ICカード701は、UIリクエスト情報送信手段707を用いてUIリクエスト情報をICカードリーダーライタ706を介して利用機702に渡し、さらに利用機702により計算機ネットワーク705を介してプロキシ装置703のUIリクエスト情報受信手段708に渡す。プロキシ装置703は、UI情報送信手段709を用いて、受信したUIリクエスト情報に基づいて生成したUI情報を計算機ネットワーク705を介して利用機702のUI情報受信手段710に渡す。

【0122】図8は本実施形態におけるUI制御処理の流れを示したフローチャートであり、図7と合わせて以下その動作を説明する。ICカード702に搭載したアプリケーションが利用機702を通じてユーザとインタラクション（入出力の受け答え）を取る場合、まずICカード702はどのようなUIを必要とするのかを情報化したUIリクエスト情報を生成する（ステップ801）。次いで、UIリクエスト情報送信手段707が前記のUIリクエスト情報を、利用機702を介してプロキシ装置703に送信する（ステップ802）。

【0123】そして、プロキシ装置703のUIリクエスト情報受信手段708がUIリクエスト情報を受け取り（ステップ803）、このUIリクエスト情報を用いて利用機におけるUI形成と動作に関わるUI情報を生成し（ステップ804）、UI情報送信手段709が利用機702に送信する（ステップ805）。

【0124】次に、利用機702のUI情報受信手段710がプロキシ装置703からUI情報を受信し（ステップ806）、このUI情報を用いてUI実行のための詳細な情報を生成する（ステップ807）。そして、利用機702が持つ画面装置、キー入力装置、ポインティング装置等のハードウェアを駆動してUIを実行する（ステップ808）。

【0125】その後、利用機702上のUIによる入出力を反映させながら、ICカード701のアプリケーションはリモートホスト704からサービスを受ける。その際、リモートホスト704との通信はプロキシ装置703を介しても良いし、利用機702が直接行っても良

い。また、ICカード701のアプリケーションが使用するサービスがプロキシ装置703までで閉じている場合は、リモートホスト704は構成要素に含める必要はない。

【0126】このように、本実施形態では、ICカード701が発するUIリクエスト情報から、プロキシ装置703内でUI情報を生成して利用機702に送り、利用機702では受信したUI情報からUIを形成し実行することにより、ICカードユーザは適切なUIを利用機上で使用できる。その際、UIリクエスト情報を送ることでICカード701に収めることのできない大容量の情報をUI情報に含むことが可能となり、その実用的効果は大きい。

【0127】[第10実施形態] 第10実施形態として、前述した第9実施形態におけるUI制御処理の具体例を示す。ICカードシステムの構成と処理の流れは第9実施形態と同様である。図9はICカードシステムにおけるUIリクエスト情報及びUI情報のデータ構造、並びにUI実行結果の一例を示す動作説明図である。

【0128】図9（A）に示すように、ICカード701のUIリクエスト情報送信手段707が発するUIリクエスト情報901は、表示位置情報902、文字属性情報903及び文字列情報904からなり、文字列情報904は文字列を構成する文字コードの配列を有し、最後の配列要素に終端記号を格納する。なお、文字列情報904は終端記号の代わりに文字列配列の先頭もしくはそれ以前に文字数を格納したデータ構造を採っても良い。

【0129】図9（B）に示すように、プロキシ装置703のUI情報送信手段709が発するUI情報905は、表示位置情報906及び画像イメージ情報907からなる。また、図9（C）はUI情報905に基づいて利用機702において実行されるUI実行結果908を示したものである。液晶表示パネル（LCD）等からなる表示画面装置909内に表示されるウィンドウ領域910において、文字列画像911が表示されている。ここで、符号912及び913は文字列画像911の表示位置であり、それぞれウィンドウ領域910の左端及び上端からの距離を用いて表される。なお、表示位置の取り方は他にも様々な方法があり、どの方法を用いても良い。

【0130】次に、本実施形態における処理の流れを説明する。図8で示した処理のステップ801で、ICカード701はUIリクエスト情報901を生成する。文字列情報904には、ICカード701のアプリケーションが利用機702を通じてユーザに見せようとする文字列の個々の文字コードを格納する。また、表示位置情報902には文字列を表示させようとする位置を示したデータを格納し、文字属性情報903には文字のフォント、色、大きさ、装飾等、表示内容を決定する際に必要

な情報を格納する。

【0131】そして、ステップ803でUIリクエスト情報901を受け取ったプロキシ装置703は、続くステップ804で、文字属性情報903と文字列情報904及びプロキシ装置が持つ文字フォントデータを用いて文字列を視覚的に表現した画像イメージ情報907を生成する。さらに、表示位置情報902を加工もしくはそのままのデータ内容で表示位置情報906を生成し、これらの画像イメージ情報907と表示位置情報906とをまとめてUI情報905を生成する。

【0132】次に、ステップ806でUI情報905を受け取った利用機702は、続くステップ807で、表示位置情報906及び画像イメージ情報907を取り出し、必要であれば利用機702自身のハードウェア及びソフトウェアの条件に適合したデータ内容に変換する。その後、ステップ807で利用機702の表示画面装置909内のウィンドウ領域910に、表示位置912、913にて文字列画像911を表示する。

【0133】なお、本実施形態では、UI情報905に含まれる画像イメージ情報907を、文字列全体を表現した単一の画像データで構成する例を示したが、画像イメージ情報907を細分化して個々の文字に対応した画像データを複数格納する方法においても同様に実施可能である。また、UIリクエスト情報901に含まれる文字列情報904には、終端記号だけでなく改行等の文字列制御情報を含むこともでき、その場合UI情報生成時もしくはUI実行時に制御情報に対応した処理を行うことで各種文字列制御が実施可能である。

【0134】また、UI情報905の生成及び受け渡し以前に、プロキシ装置703が利用機702に対して、使用しようとするフォントデータを持っているかどうかを問い合わせ、持っていない場合は上記のように画像データとして送り、既に持っている場合は文字コードを送る、という方法も実施可能である。また、本実施形態では利用機702のUI実行手段711として表示画面装置909を適用した例で説明したが、その他プリンタなどの印刷装置等についても同様に実施可能である。

【0135】このように、本実施形態では、UIリクエスト情報901に文字コードを含め、UI情報905に文字コードに対応した画像イメージを含めることにより、利用機702が持っていない文字フォントによる文字情報であっても、ICカード701からのリクエストにより使用可能となる。さらにICカード701にフォントデータを置くことなく実現することができるので、ICカード701において大量の文字情報を格納しておく必要がなく、データ記憶容量を削減でき、その実用的効果は大きい。

【0136】〔第11実施形態〕第11実施形態として、前述した第9実施形態におけるUI制御処理の第1の変形例を示す。ICカードシステムの構成と処理の流

れは第9実施形態と同様である。第11実施形態では、UI情報には、利用機702のハードウェアを利用してユーザインタフェースとして動作させるためのプログラム情報を適用し、UIリクエスト情報には前記のプログラムが実行時に使用するパラメータ情報を適用する。UI情報にはプログラム情報の他に任意のデータ情報を含むこともでき、また、UIリクエスト情報によって前記データ情報もしくはプログラム情報自体を動的に生成しても良い。

10 【0137】本実施形態の場合、図8のフローチャートにおいては、ステップ806で利用機702に渡されたUI情報は、ステップ808でUI実行手段711によってプログラムとして解釈され、実行される。

【0138】ここで、UIリクエスト情報を、利用機701の表示画面装置上に表示する文字、ボタン、入力領域等のユーザインタフェース部品の情報から構成し、UI情報をこれらのユーザインタフェース部品を配置し駆動するプログラムとすることにより、ICカード701のアプリケーションが意図する様々なユーザインタフェースを利用機702上で実行することができる。プログラムの構成は、利用機702のハードウェアに依存した機械語コードを用いるか、もしくは利用機702に特定の言語のインタプリタもしくはプログラムを実行する仮想マシンを搭載し、それらの上で動作するプログラムコードを適用する。

【0139】このように、第11実施形態によれば、UI情報としてプログラム情報を適用することにより、利用機702上で柔軟なユーザインタフェースを実行することができ、その実用的効果は大きい。

30 【0140】〔第12実施形態〕第12実施形態として、前述した第9実施形態におけるUI制御処理の第2の変形例を示す。ICカードシステムの構成と処理の流れは第9実施形態と同様である。また、UI情報としてプログラム情報を適用する点において第11実施形態と同様である。

【0141】第12実施形態では、図8のフローチャートにおけるステップ804でUI情報を生成する前に、プロキシ装置703が保持する利用機702に関する情報を用いるか、もしくはプロキシ装置703が利用機702に問い合わせを行うことによって利用機702の構成等の情報を獲得し、それに基づいてUI情報に含まれるプログラムの内容を異なるものにする。

40 【0142】例えば、利用機702が持つ表示画面装置の大きさや解像度に応じて、ユーザインタフェース部品の配置や大きさを変更したり、入力装置の種類によって異なるユーザインタフェース部品を配置したりすることができる。

【0143】このように、第12実施形態によれば、UI情報として用いるプログラム情報を利用機702の条件に基づいて異なるものにするにより、利用機70

2が様々な種類の構成要素からの選択により構成される場合でも適切なユーザインタフェースを得ることが可能となり、その実用的効果は大きい。

【0144】[第13実施形態] 図10は本発明の第13実施形態に係るICカードシステムの構成を示すブロック図である。第13実施形態は、第1実施形態と同様に、ICカード1001、利用機1002、プロキシ装置1003、リモートホスト1004を有して構成され、利用機1002とプロキシ装置1003、及びプロキシ装置1003とリモートホスト1004はそれぞれ計算機ネットワーク1005を介して接続される。利用機1002はICカードリーダーライタ1006を具備している。これら各構成装置の基本的な構成と関係は図1の第1実施形態と同様である。

【0145】ICカード1001は、利用機1002と通信を行って利用機1002の認証と識別を行う利用機認証手段1007と、利用機認証手段1007の動作結果を基に利用機1002の信頼度がいかなるものであるかの評価を行う利用機評価手段1008と、暗号化処理を行う暗号処理手段1009とを備えている。

【0146】また、プロキシ装置1003は、ICカード1001に対応して、暗号化処理を行う暗号処理手段1010と、利用機1002の信頼度評価を行う利用機評価手段1011とを備えている。ICカード1001の暗号処理手段1009とプロキシ装置1003の暗号処理手段1010は対になって情報秘匿を行い、両者間にセキュアパス1012を形成する。セキュアパス1012形成についての処理手順は第5実施形態と同様であり、詳細説明は省略する。

【0147】図11は本実施形態における利用機の信頼度評価処理の流れを示したフローチャートであり、図10と合わせて以下その動作を説明する。ここでは、ICカード1001とプロキシ装置1003が利用機1002の信頼度評価結果を共有する場合の処理を例示する。

【0148】まず、ICカード1001の利用機認証手段1007が利用機1002の認証もしくは識別を行い、利用機1002が何者であるかを特定する(ステップ1101)。その際、利用機1002の固有情報を得てICカード1001が保持する情報と照らし合わせて認証を行う方法、またはICカード1001と利用機1002の間で通信を行い、パスワード情報等をやり取りして認証を行う方法等が挙げられるが、基本的に識別及び認証の方法には依存するものではない。既知の技術をもって利用機の識別及び認証を実施可能である。

【0149】そして、利用機認証結果を基に、利用機評価手段1008が利用機の信頼度を評価し、利用機1002が予め定めたセキュリティポリシー上の分類に基づいてどの程度の信頼度であるのかを算出する(ステップ1003)。例えば、利用機の信頼度のカテゴリを3段階に分け、「完全に安全」「ほぼ安全」「安全でない」と

評価する例で考えると、利用機評価手段1008はこの3つの状態を数値等の識別可能なデータをもって利用機評価結果とする。さらに具体的な細分化の例として、「利用機運用者による不正行為の可能性」「通りがかりの人間による不正行為の可能性」「ネットワーク経由の不正行為の可能性」をそれぞれ予測して、各項目の有無のマトリクスにより利用機を細かいカテゴリに分類する方法が挙げられる。この場合、それぞれの不正行為の可能性の有無によって、いかなる脅威が存在するかを想定することが可能であり、その想定を基にセキュリティポリシーを立てれば良い。

【0150】次に、セキュアパス1012を用いて、ICカード1001はプロキシ装置1003に利用機評価結果を渡し(ステップ1104)、プロキシ装置1003が持つ利用機評価手段1011がこれを受けて、ICカード1001が持つ利用機評価手段1008と利用機1002の信頼度評価結果を共有する。その後、プロキシ装置1003は信頼度評価結果に基づいて予め定めた規則に従って通信内容等を設定し、利用機1002との通信を行う。同様にリモートホスト1004との通信も行いが、本実施形態においては必ずしもリモートホスト1004は必要としない。なお、利用機評価手段1008が獲得する利用機評価結果のデータは、上記の例に限らず様々な形態で実施する。

【0151】このように、第13実施形態では、利用機1002を認証もしくは識別した結果から利用機1002の信頼度を評価し、その結果をICカード1001からプロキシ装置1003にセキュアパス1012を介して渡すことにより、利用機1002の信頼度をICカード1001とプロキシ装置1003の両者が共有することができ、利用機1002やリモートホスト1004に対するその後の通信に反映させることができる。これは主に、ICカード1001もしくはプロキシ装置1003が、不用意に渡してはならない情報を利用機1002に漏らしてしまうことを防止する作用に反映させることができ、信頼度に応じたセキュリティを確保した適切な情報の送受信が可能となり、その実用的効果は大きい。

【0152】[第14実施形態] 図12は本発明の第14実施形態に係るICカードシステムの構成を示すブロック図である。第14実施形態は第13実施形態の変形例であり、プロキシ装置側に利用機認証手段等を設けたものである。図12の各構成要素において、符号1201～1206は図10における1001～1006に、符号1209～1211は図10における1009～1011にそれぞれ対応している。

【0153】第13実施形態と異なるのは、プロキシ装置1203に利用機認証手段1207と利用機評価手段1208が設けられることであり、利用機認証結果共有時のデータの流れが第13実施形態と逆方向になる。図13は本実施形態における利用機の信頼度評価処理の流

れを示したフローチャートである。この図 13 のステップ 1301~1304 において、IC カードと利用機の役割が入れ替わる他は、図 11 のステップ 1101~1104 と処理手順は同様である。

【0154】このように、プロキシ装置 1203 が利用機 1202 を認証、識別し、信頼度の評価結果を IC カード 1201 に渡すことにより、第 13 実施形態と同様に、信頼度の情報をプロキシ装置と IC カードで共有することが可能となる。ただし、第 14 実施形態においてはプロキシ装置 1203 が利用機 1202 を認証すること

ことができ、IC カード 1201 が認証する場合と比較して強力かつ綿密な認証、識別及び信頼度評価が可能となるため、より一層セキュリティの強化を図ることができる。【0155】[第 15 実施形態] 第 15 実施形態は、第 14 実施形態のさらなる変形例を示したものである。IC カードシステムの構成及び処理の流れはそれぞれ図 12 及び図 13 と同様である。第 15 実施形態では、プロキシ装置 1203 の利用機認証手段 1207 がステップ 1301 で利用機 1202 を認証する際に、計算機ネットワーク 1205 における利用機 1202 の固有情報を用いる。例えば、計算機ネットワーク 1205 がインターネット等の TCP/IP を通信プロトコルとして用いるネットワークの場合、前記固有情報として IP アドレスが利用できる。利用機認証手段 1207 は、利用機 1202 の IP アドレスを元に認証、識別を行う。

【0156】このように、第 15 実施形態では、計算機ネットワーク 1205 に関連する利用機 1202 の固有情報を用いることにより、利用機の認証や識別が容易にかつ確実にでき、所望のセキュリティを確保した IC カードシステムの運用が簡便に実現可能であるため、その実用的効果は大きい。

【0157】[第 16 実施形態] 図 14 は本発明の第 16 実施形態に係る IC カードシステムの構成を示すブロック図である。第 16 実施形態は、前述した第 13 実施形態に要素を追加した形で構成される。

【0158】すなわち、第 13 実施形態と同様に、IC カード 1401、利用機 1402、プロキシ装置 1403、リモートホスト 1404 を有して構成され、利用機 1402 とプロキシ装置 1403、及びプロキシ装置 1403 とリモートホスト 1404 はそれぞれ計算機ネットワーク 1405 を介して接続される。そして、IC カード 1401 は利用機認証手段 1407、利用機評価手段 1408 及び暗号処理手段 1409 を備え、プロキシ装置 1403 は利用機認証手段 1412、利用機評価手段 1413 及び暗号処理手段 1410 を備えており、暗号処理手段 1409 と 1410 との間でセキュアパス 1411 を形成する。なお、図に示した例では利用機認証手段は 1407 と 1412 の 2 つが存在するが、これらは少なくとも片方が備えられていれば良い。

【0159】また、IC カード 1401 は送信情報制御手段 1414 を備え、この送信情報制御手段 1414 により、利用機評価手段 1408 の動作結果を基にして IC カード 1401 から利用機 1402 に送信するデータ内容を制御する。すなわち、利用機 1402 の信頼度の高低に応じて、もしくは第 13 実施形態で示したように信頼度の要素がマトリクス上に細分化されている場合は個々のセキュリティポリシーに照らして、適切なデータを送信する。その最も単純な例は、利用機評価結果を「信頼できる」「信頼できない」の 2 値とし、「信頼できない」場合には「機密」に分類されたデータを一切送信しないことである。

【0160】このように、第 16 実施形態では、IC カード 1401 の利用機評価手段 1408 の動作結果を用いて送信情報制御手段 1414 が利用機 1402 の信頼度に応じたデータを送信することにより、柔軟かつ強力なセキュリティを得ることができ、その実用的効果は大きい。この場合、IC カード側で信頼度を判断して送信データの内容を制御することが可能である。

【0161】[第 17 実施形態] 第 17 実施形態は前述した第 16 実施形態の送信情報制御に関する第 1 の例であり、IC カードシステムの構成は図 14 と同様である。第 17 実施形態では、利用機評価手段 1408 の動作結果を基に利用機 1402 の信頼度の高低を評価した結果が「信頼できない」と判断される場合に、IC カード 1401 のアプリケーションが利用機 1402 に送信しようとしていたデータについて、送信前に送信情報制御手段 1414 が処理し、セキュリティポリシー上利用機 1402 に対して漏らすべきでない情報を削除する。これにより、利用機 1402 毎の信頼度に応じた情報秘匿が可能となる。なお、信頼度評価結果を多値とし、各々の信頼度の値に従って異なる方法でデータから情報の一部もしくは全部を削除する方法でも同様に実施可能である。

【0162】[第 18 実施形態] 第 18 実施形態は前述した第 16 実施形態の送信情報制御に関する第 2 の例であり、IC カードシステムの構成は図 14 と同様である。第 18 実施形態では、送信情報制御手段 1414 は、IC カード 1401 が保持する機密情報を送信前にチェックし、利用機評価手段 1408 が利用機 1402 を「信頼できない」と判断した場合には、機密情報を送信データから削除もしくは他のデータに変更する。これにより、IC カード 1401 が保持する機密情報の秘匿を利用機 1402 毎の信頼度に応じて行うことが可能となる。

【0163】[第 19 実施形態] 第 19 実施形態は前述した第 16 実施形態の送信情報制御に関する第 3 の例であり、IC カードシステムの構成は図 14 と同様である。第 19 実施形態では、送信情報制御手段 1414 は、IC カード 1401 が保持する IC カード 1401

のユーザのプライバシーに関わる情報を送信前にチェックし、利用機評価手段1408が利用機1402を「信頼できない」と判断した場合には、プライバシー情報を送信データから削除もしくは他のデータに変更する。これにより、ICカード1401が保持するプライバシー情報の秘匿を利用機1402毎の信頼度に応じて行うことが可能となる。

【0164】 [第20実施形態] 図15は本発明の第20実施形態に係るICカードシステムの構成を示すブロック図である。第20実施形態は、前述した第14実施形態に要素を追加した形で構成される。

【0165】 すなわち、第14実施形態と同様に、ICカード1501、利用機1502、プロキシ装置1503、リモートホスト1504を有して構成され、利用機1502とプロキシ装置1503、及びプロキシ装置1503とリモートホスト1504はそれぞれ計算機ネットワーク1505を介して接続される。そして、ICカード1501は利用機認証手段1507、利用機評価手段1508及び暗号処理手段1509を備え、プロキシ装置1503は利用機認証手段1512、利用機評価手段1513及び暗号処理手段1510を備えており、暗号処理手段1509と1510との間でセキュアパス1511を形成する。なお、図に示した例では利用機認証手段は1507と1512の2つが存在するが、これらは少なくとも片方が備えられていれば良い。

【0166】 この第20実施形態は、第16実施形態と比較した場合、送信情報制御手段1514をICカード1501ではなくプロキシ装置1503側に設けた点が構成上異なる。この送信情報制御手段1514により、利用機評価手段1513の動作結果を基にしてプロキシ装置1503から利用機1502に送信するデータ内容を制御する。すなわち、利用機1502の信頼度の高低に応じて、セキュリティポリシー上好ましい状態のデータを送信する。

【0167】 このように、第20実施形態では、第16実施形態と同様に、プロキシ装置1503の利用機評価手段1513の動作結果を用いて送信情報制御手段1514が利用機1502の信頼度に応じたデータを送信することにより、柔軟かつ強力なセキュリティを得ることができ、その実用的効果は大きい。この場合、ICカード側で利用機の信頼度がわからなくても、プロキシ装置側で信頼度を判断して送信データの内容を制御することが可能である。

【0168】 [第21実施形態] 第21実施形態は前述した第20実施形態の送信情報制御に関する第1の例であり、ICカードシステムの構成は図15と同様である。第21実施形態では、利用機評価手段1513の動作結果を基に利用機1502の信頼度の高低を評価した結果が「信頼できない」と判断される場合に、プロキシ装置1503のアプリケーションが利用機1502に送

信しようとしていたデータについて、送信前に送信情報制御手段1514が処理し、セキュリティポリシー上利用機1502に対して漏らすべきでない情報を削除する。これにより、利用機1502毎の信頼度に応じた情報秘匿が可能となる。なお、信頼度評価結果を多値とし、各々の信頼度の値に従って異なる方法でデータから情報の一部もしくは全部を削除する方法でも同様に実施可能である。

【0169】 [第22実施形態] 第22実施形態は前述した第20実施形態の送信情報制御に関する第2の例であり、ICカードシステムの構成は図15と同様である。第22実施形態では、送信情報制御手段1514は、プロキシ装置1503が保持する機密情報を送信前にチェックし、利用機評価手段1513が利用機1502を「信頼できない」と判断した場合には、機密情報を送信データから削除もしくは他のデータに変更する。これにより、プロキシ装置1503が保持する機密情報の秘匿を利用機1502毎の信頼度に応じて行うことが可能となる。

【0170】 [第23実施形態] 第23実施形態は前述した第20実施形態の送信情報制御に関する第3の例であり、ICカードシステムの構成は図15と同様である。第23実施形態では、送信情報制御手段1514は、プロキシ装置1503が保持するICカード1501のユーザのプライバシーに関わる情報を送信前にチェックし、利用機評価手段1513が利用機1502を「信頼できない」と判断した場合には、プライバシー情報を送信データから削除もしくは他のデータに変更する。これにより、プロキシ装置1503が保持するICカードユーザのプライバシー情報の秘匿を利用機1502毎の信頼度に応じて行うことが可能となる。

【0171】 [第24実施形態] 図16は本発明の第24実施形態に係るICカードシステムの構成を示すブロック図である。第24実施形態は、第1実施形態と同様に、ICカード1601、利用機1602、プロキシ装置1603、リモートホスト1604を有して構成され、利用機1602とプロキシ装置1603、及びプロキシ装置1603とリモートホスト1604はそれぞれ計算機ネットワーク1605を介して接続される。利用機1602はICカードリーダライタ1606を具備している。これら各構成装置の基本的な構成と関係は図1の第1実施形態と同様である。

【0172】 ICカード1601は利用機認証手段1607、利用機評価手段1608、暗号処理手段1609を、プロキシ装置1603は利用機認証手段1612、利用機評価手段1613、暗号処理手段1610をそれぞれ備えており、暗号処理手段1609と1610との間でセキュアパス1611を形成する。これらの手段の基本的構成は前述した第13、第14、第16、及び第20実施形態と同様である。



【0173】また、ICカード1601はUIリクエスト情報送信手段1615を備え、プロキシ装置1603はUIリクエスト情報受信手段1616とUI情報送信手段1617を備え、利用機1602はUI情報受信手段1618とUI実行手段1619を備えている。これらの手段の基本的構成は前述した第9及び第10実施形態と同様である。

【0174】さらに、本実施形態では、プロキシ装置1603は送信情報制御手段1614を備えている。利用機評価手段1613により得られる利用機1602の信頼度に応じて、UI情報送信手段1617が利用機1602のUI情報受信手段1618にデータを送る前に、信頼度が低い場合は送信情報制御手段1614が作用してデータの変更、制限を行う。

【0175】図17は本実施形態におけるUI実行処理の流れを示したフローチャートであり、図16と合わせて以下その動作を説明する。まず、ICカード1601とプロキシ装置1603が利用機1602の信頼度情報を共有する(ステップ1701、ステップ1702)。この信頼度情報共有のための処理手順は第13及び第14実施形態に示した通りである。そして、ICカード1601に搭載したアプリケーションが生成したUIリクエスト情報を送信し、これをプロキシ装置1603が受け取り、それを基にUI情報を生成する(ステップ1703~1706)。この間の処理手順は第9実施形態に示した通りである。

【0176】次に、プロキシ装置1603の利用機評価手段1613が、利用機1602の信頼度を評価する(ステップ1707)。ここでは、信頼度評価結果の例として「信頼できる」「信頼できない」の2値評価を適用する。「信頼できる」と評価した場合は、生成されたUI情報をそのまま利用機1602に送信する(ステップ1709)。一方、「信頼できない」と評価した場合は、ステップ1709に進む前に、送信情報制御手段1604がUI情報に変更を加え、ユーザインタフェースに制限を掛け(ステップ1708)、その後ステップ1709に進む。

【0177】そして、利用機1602は受信したUI情報を基にUI実行のための情報を形成し、具備しているハードウェアを駆動してUIを実行する(ステップ1710~1712)。このステップ1709~1712に至る処理手順は第9実施形態に示した通りである。

【0178】図18はUIリクエスト情報の一例を示す動作説明図である。この例では、UIリクエスト情報1800は、表示コマンド1801と表示属性1802及び表示対象配列1803の3種類のデータの複合情報から成る。表示コマンド1801はUIリクエスト情報1801の求めるUI動作を識別するためのデータであり、表示属性1802は表示位置、文字指定、文字属性その他の表示に関わる情報を含んだデータである。表示

対象配列1803は表示する対象となるデータを特定するための情報を複数収めた配列データである。

【0179】表示対象配列1803の各要素として、この例ではユーザ氏名情報1804、住所情報1805、電話番号情報1806、勤務先情報1807、口座番号情報1808、口座残高情報1809、取引履歴情報1810を格納する。これらの各要素情報1804~1810には、例えば氏名であれば氏名を表現した文字列データそのものを入れても良いし、またはプロキシ装置1603が氏名の文字列を得ることができるような識別情報を入れても良い。ただし、この情報が氏名に関わるものであることを、プロキシ装置1603が認識できるための情報が含まれている必要がある。

【0180】なお、これらのUIリクエスト情報のデータ構造はあくまで一例であり、他の様々な方法によって類似する情報内容を構成し得る。

【0181】上記のUIリクエスト情報1800を、図17に示したステップ1704~1705でICカード1601からプロキシ装置1603に伝送する際、原則としてセキュアパス1611を介するのが好ましい。ただし、UIリクエスト情報に含まれる情報から機密に関わる情報を直接もしくは間接的に利用機1602が得ることができないことが分かっている場合は、セキュアパス1611以外の手段を用いて伝送しても良い。

【0182】図19は、UI情報及びUI実行結果の第1の例として、利用機が「信頼できる」と評価された場合を示す動作説明図である。これは、プロキシ装置1603の利用機評価手段1613が、図17のステップ1707において利用機1602を「信頼できる」と評価した場合である。

【0183】図19(A)に示すUI情報1901は、上述したように図17のステップ1706にて生成される。UI情報1901の内容は、個々の表示対象に対して、それが文字表示であることを表すコマンド情報1902、表示時の詳細な制御内容(表示属性)を表す属性情報1903を、それぞれ表示対象データ1904~1910と組にして一まとめにしたものである。表示対象データ1904~1910には、例えば氏名であれば氏名を表す文字列情報が直接含まれ、それらは文字コードもしくは文字を表現する画像データから構成される。

【0184】このUI情報1901は、利用機1602のUI実行手段1619によって解釈されるデータもしくはプログラムとして扱うことができる。なお、UI情報に関してもUIリクエスト情報と同じく、本実施形態で挙げた例の他に様々な方法によって構成し得る。

【0185】この第1の例のように、利用機1602が「信頼できる」場合、UI実行結果は図19(B)に示すようになる。すなわち、表示対象データ1904~1910に対応する全てのデータ内容が、UI実行結果1911として利用機1602の表示画面装置等に表示出

力される。

【0186】図20は、UI情報及びUI実行結果の第2の例として、利用機が「信頼できない」と評価された場合を示す動作説明図である。これは、プロキシ装置1603の利用機評価手段1613が、図17のステップ1707において利用機1602を「信頼できない」と評価した場合である。

【0187】この場合、ステップ1708で送信情報制御手段1614が作用し、図20(A)に示すUI情報2001のように、機密に関わる表示対象データである口座番号データ1908、口座残高データ1909、取引履歴データ1910を、それぞれダミーデータ2002~2004に書き換える。

【0188】この第2の例では、図20(B)に示すように、UI実行結果2005は機密に関わる個々のデータはダミーデータとして「X」などに置き換えられ、隠匿された状態で利用機1602の表示画面装置等に表現されるので、画面表示内容を搾取されたり印刷内容を盗用されたりした場合でも、機密が漏洩することを防げる。また、UI情報2001そのものにもこれらの機密情報が含まれていないため、不正な手段を用いてUI情報を解析したとしても、機密の漏洩を防止できる。

【0189】なお、本実施形態では、利用機評価手段1613による信頼度評価を2値評価とした例で説明したが、評価結果を細分化して多値評価を行い、それに応じてステップ1708における処理を多岐に分ける方法を探っても実施可能である。これをUI情報及びUI実行結果の第3の例として、上記第2の例とは異なる条件での機密管理の実行例を図21に示す。

【0190】図21は、UI情報及びUI実行結果の第3の例として、利用機が「さらに信頼できない」と評価された場合を示す動作説明図である。この第3の例では、図20の場合よりも「さらに信頼できない」利用機を想定しており、UI情報2101は、口座に関する情報はもとより、ユーザの住所、電話番号、勤務先情報まで機密としてダミーデータに書き換え、利用機1602に漏洩しないようにしている。この場合のUI実行結果2102は、ユーザの氏名情報以外は全てダミーデータとして「X」などに置き換えられて利用機1602の表示画面装置等に表示される。

【0191】このように、利用機評価手段1613の評価結果に基づいて利用機1602上で実行されるUIに変更を掛けて表示する情報を制限することにより、利用機1602の信頼度が低い場合に、表示画面装置等に表示された情報が搾取されたりしても機密情報を盗み取られるおそれがなくなり、その実用的効果は極めて高い。この第24実施形態によって、[発明が解決しようとする課題]の欄に示した第2の問題点のうち、画面出力、印刷出力等のユーザへの出力内容から機密が漏洩する問題を明確に解決することができる。

【0192】[第25実施形態] 第25実施形態はUI制御処理の他の例を示したものである。ICカードシステムの構成と処理の流れは第24実施形態と同様である。この実施形態は、UI実行の内容が表示ではなく、入力に関わる点が第24実施形態と異なる。

【0193】図22はUIリクエスト情報及びUI実行結果の例を示す動作説明図である。図22(A)に示すように、UIリクエスト情報2201は、文字入力をもとにUIを得るための入力コマンド情報2202、文字入力に関する属性情報2203、入力対象要素であるユーザ名2205及びパスワード2206からなる入力対象配列2204、入力ボタンのUIを得るためのボタンコマンド情報2207、ボタンに関する属性情報2208、ボタン要素である公開情報2210及び秘密情報2211からなるボタン配列2209を含んでいる。このUIリクエスト情報2201は、ユーザ名、パスワードを入力する2つの文字入力フィールドと、公開情報、秘密情報を得るための2つのボタンを入力部品としたUIを利用機1602上で実行することを要求するものである。

【0194】このUIリクエスト情報2201に対して第24実施形態と同様の処理を行い、利用機1602の信頼度評価結果に応じて異なるUI情報を用意する。ここで、利用機1602が「信頼できる」場合は図22(B)に示すようなUI実行結果2212が、「信頼できない」場合は図22(C)に示すようなUI実行結果2213がそれぞれ得られる。すなわち、「信頼できる」場合は要求された全ての入力部品が利用機1602上で実行されて表示され、「信頼できない」場合はパスワード入力フィールド及び秘密情報ボタンがUIの表示から削除される。

【0195】これにより、利用機1602の信頼度が低い場合は機密情報入力用のUIが表示されないため、ユーザは機密に関わる情報を利用機1602上の機器を用いて入力することができなくなり、機密情報の漏洩が防止できる。特に、パスワード入力についてはキー入力の状態を搾取することによるパスワード盗用を防ぐことが可能であり、その実用的効果は極めて大きい。

【0196】次に、第24実施形態と第25実施形態を複合的に適用したウェブメール、即ちWWWの仕組みを利用した個人向け電子メールサービスの具体例を示す。ウェブメールを読むためのWWWブラウザに相当するアプリケーションをICカードが持ち、このアプリケーションは利用機を通じてウェブメールサーバ(ウェブメールサービスを行うリモートホスト)にアクセスする。この時、第2実施形態及び第4実施形態に示したアクセス先情報秘匿を適用すれば、利用機に対してウェブメールサーバの所在を隠すこともできる。

【0197】ICカードのアプリケーションは、ウェブメールサーバからICカードユーザの受信メール一覧を

取得し、UI リクエスト情報をプロキシ装置に送る。プロキシ装置はUI リクエスト情報に基づいてUI 情報を構築するが、その際利用機評価手段の作用によって利用機を「信頼できる」と判断した場合はUI 情報には全ての受信メールの見出し情報と、メール本文を読むためのボタン(WWWのリンク)を含んだままとする。一方、利用機を「信頼できない」と判断した場合には、受信メールのうち機密と分類されるものについての見出し情報を隠し(あるいは他の非機密情報に変更し)、さらにメール本文を読むためのボタンも含まないようにする。

【0198】図23は「信頼できる」利用機を使用した場合のUI 実行結果の一例を、図24は「信頼できない」利用機を使用した場合のUI 実行結果の一例をそれぞれ示したものである。

【0199】図23に示すように、信頼できる利用機の場合は、全ての受信メールの差出人、送信日時及びサブジェクト(メールのタイトル)が表示され、さらにそれらがWWWのリンクとなり、ユーザはそのリンクを指定する(タッチパネルでクリックもしくはポインティングデバイスでリンクの場所にポインタを合わせてボタン等で指定する)ことで、それらのメールの本文を読むことができる。しかし、図24に示すように、信頼できない利用機の場合は、例えばサブジェクトに「機密」もしくは「SECRET」という文字列が含まれるメールを全て機密文書とみなし、そのメールに関する一切の情報を表示させないようにしている。もちろん本文も読むことはできない。

【0200】上記の例では、機密文書の判断基準として単純にサブジェクトに含まれる文字列のみを用いたが、他に、差出人による判断、メールのヘッダによる判断、もしくはメール本文を先に(利用機に表示することなく)解析して機密にあたる情報が含まれるか否かを判断する等の方法が考えられる。また、上記の例ではWWWブラウザに相当するアプリケーションをICカードに搭載するようにしたが、これを利用機に持たせ、ICカードはプロキシ装置と連携してウェブメールサーバから得る情報に制限を加える方法でも実施可能である。

【0201】いずれにしても、本実施形態によって、[発明が解決しようとする課題]の欄に示した第2の問題点を明確に解決することができる。本実施形態では機密情報の入力そのものを不可とするため、暗証番号やパスワードを要求するリモートホストのサービスは受けることができないが、機密情報漏洩に対しては強力な効果を発揮するものである。

【0202】[第26実施形態] 図25は本発明の第26実施形態に係るICカードシステムの構成を示すブロック図である。第26実施形態は、第1実施形態と同様に、ICカード2501、利用機2502、プロキシ装置2503、リモートホスト2504を有して構成され、利用機2502とプロキシ装置2503、及びプロ

キシ装置2503とリモートホスト2504はそれぞれ計算機ネットワーク2505を介して接続される。利用機2502はICカードリーダライタ2506を具備している。これら各構成装置の基本的な構成と関係は図1の第1実施形態と同様である。

【0203】ICカード2501は、利用機を通じてユーザが入力したデータ(仮の機密情報)を基に、別のデータ(真の機密情報)を生成する機密情報変換手段2507を備える。また、図示しないが、ICカード2501およびプロキシ装置2503はそれぞれ暗号処理手段を備えており、これらの暗号処理手段と利用機2503が持つデータ転送手段との組み合わせでセキュリティを確保したデータ通信経路としてセキュアパス2508が形成される。このセキュアパス2508は前述した実施形態と同様であり、ここでは説明を省略する。なお、機密情報変換手段2507は、ICカード2501ではなくプロキシ装置2503が備える構成としても良い。その場合にはセキュアパス2508は不要である。

【0204】利用機2502はUI 実行手段2509を備えている。このUI 実行手段2509は、前述の第9～第25実施形態で示したものの他、利用機2502自身の処理作用による一般的なUI も含むことができる。プロキシ装置2503は、ICカード2501の機密情報変換手段2507から機密情報を受け取る機密情報獲得手段2510を備えている。なお、この機密情報獲得手段2507をプロキシ装置2503が備える場合には、機密情報変換手段2507と一体化しても良い。

【0205】リモートホスト2504は機密情報要求手段2511を備えている。この機密情報要求手段2511は、リモートホスト2504が提供するサービスにおいて暗証番号やパスワードの入力を要求する一般的な事物を表す。ここで、機密情報要求手段2511が求める情報を、真の機密情報と呼ぶことにする。即ち、リモートホスト2504のサービスを利用しようとする者は、真の機密情報を機密情報要求手段2511に渡すことで、初めて利用のための権限が与えられる。

【0206】図26は本実施形態における機密情報保護処理の流れを示したフローチャートであり、図25と合わせて以下その動作を説明する。まず、ICカード2501のユーザは、利用機2502のUI 実行手段2509を用いて真の機密情報を得るためのキーとなる情報を入力する(ステップ2601)。以下、この情報を仮の機密情報と呼ぶことにする。なお、仮の機密情報そのものには機密性はなく、これを搾取してリモートホスト2504のサービスを受けることはできないようになっている。次に、利用機2502は仮の機密情報をICカード2501に送信し、ICカード2501はこれを受信する(ステップ2602、ステップ2603)。ICカード2501の機密情報変換手段2507は、受信した仮の機密情報を元に演算を行い、真の機密情報を生成す

る（ステップ2604）。

【0207】仮の機密情報から真の機密情報を生成する方法の例としては、予め定めたキーワード（合い言葉）を仮の機密情報とし、ユーザが入力したキーワードから、それに対応する情報を登録済みの情報から検索して真の機密情報とする方法、あるいは予め定めた変換方法に従って真の機密情報を変換したものを仮の機密情報として、ユーザが入力したデータに逆変換を掛けて真の機密情報を得る方法、等が挙げられる。前者はユーザが覚えやすいキーワードを用いることで使用が簡単になる反面、予め登録しておかなかった真の機密情報は扱えないという特徴がある。後者は任意の情報を生成することが容易であり、特に文字列による機密情報の入力を行う際に適するが、その反面、変換規則をユーザが把握し、自ら何らかの手段を用いて変換データを用意する必要がある、難解になり易い特徴がある。また、いずれの場合にも仮の機密情報から真の機密情報を容易に類推されないことが重要である。

【0208】機密情報変換手段2507で真の機密情報を生成した後、ICカード2501はセキュアパス2508を通じて真の機密情報をプロキシ装置2503の機密情報獲得手段2510に渡す（ステップ2605、ステップ2606）。最後に、プロキシ装置2503は真の機密情報をリモートホスト2504の機密情報要求手段2511に渡す（ステップ2607）。

【0209】なお、機密情報変換手段2507をプロキシ装置2503が備える場合には、上記のステップ2602において仮の機密情報は利用機2502からプロキシ装置2503に渡され、ステップ2603及びステップ2604の機密情報変換はプロキシ装置2503内で処理される。またこの場合、ステップ2605とステップ2606は不要となり、プロキシ装置2503はステップ2604にて生成した真の機密情報をそのままステップ2607にてリモートホスト2504に渡せば良い。

【0210】図27は、本実施形態を適用したUI実行結果であるパスワード入力UIの画面例と、パスワード情報としてリモートホストに渡されるデータの具体例を示した動作説明図である。図27において、(A)は利用機上に表示されるUI画面表示例、(B)は仮の機密情報をパスワードとして入力した状態のUI画面表示例、(C)は真の機密情報と仮の機密情報の一例をそれぞれ示す。この場合、ユーザからは真の機密情報（正パスワード）である文字列“mYReAlpassWORD”の代わりに、仮の機密情報（仮パスワード）である文字列“tempasswd1”が利用機2502に与えられる。そして、文字列“tempasswd1”は機密情報変換手段2507によって文字列“mYReAlpassWORD”に変換され、パスワードとしてリモートホスト2504に渡される。

【0211】このように、第26実施形態では、機密情

報をユーザが直接に利用機2502に与える代わりに仮の機密情報を入力し、それをICカード2501の機密情報変換手段2507で真の機密情報に変換してセキュアパス2508を通じてプロキシ装置2503に渡すことで、機密方法を利用機2502に秘匿した状態でリモートホスト2504へ渡すことができる。即ち、ウェブメール、オンラインショッピング等、アクセスパスワードの入力が必要なサービスを、ICカードのユーザが利用機にパスワードを漏洩させることなく利用することが可能となり、その実用的効果は極めて大きい。この実施形態によって、[発明が解決しようとする課題]の欄に示した第2の問題点のうち、キーボード、タッチパネル等の入力手段によるユーザからの入力内容から機密が漏洩する問題を明確に解決することができる。また、第26実施形態では、第25実施形態のように機密情報を秘匿するものとは異なり、機密情報を変換して受け渡すことで暗証番号やパスワードを要求するリモートホストのサービスを受けることが可能である。

【0212】[第27実施形態] 第27実施形態は前述した第26実施形態の機密情報保護に関する第1の変形例であり、ICカードシステムの構成及び処理の流れは第26実施形態と基本的に同様である。この例は、機密情報変換手段2507が行う変換処理のためのデータを、ユーザによる仮の機密情報入力に先立って装置からユーザに提示する点が異なる。

【0213】図28はUI実行結果として利用機上に表示されるUI画面とそこに情報を入力した状態の具体例を示す動作説明図である。この場合、利用機2502のUI実行手段2509によってパスワード入力に関する情報がユーザに提示され、それを受けてユーザが仮の機密情報である仮パスワードを入力する。パスワードを入力するUI部品には、パスワード入力領域に付随して、変換キーを表示する領域を設ける。変換キーは機密情報変換手段2507が変換処理に使用するパラメータであり、変換キーが違えば真の機密情報として同一の結果を得るための仮の機密情報は異なるように、変換キー毎に仮の機密情報を設定する必要がある。ここでは変換キーとして“12”という数字を用いているが、この数字はユーザが利用機を使用する毎に異なる値にすることが必要で、乱数を用いることが望ましい。

【0214】ユーザは、図26に示したステップ2601において、変換キーの内容を考慮して、真の機密情報に正しく変換される文字列を仮の機密情報として入力する。それ以降の処理は第26実施形態と同様である。ただし、この場合、ステップ2604において機密情報変換手段2507が真の機密情報を生成する際に、ユーザに提示した変換キーと同一のデータを用いて変換処理を行うことが必須である。このようなランダムデータを用いた機密情報の入力は、動的認証（ダイナミックオーセンティケーション）技術として一般に知られているが、

本実施形態は、機密情報を要求するリモートホスト 2504 が動的認証を行わない場合においても適用可能である点と、ランダムデータの提示を含む UI を、第 9 ～ 第 25 実施形態で示した UI 情報の形成方法を用いてプロキシ装置 2503 が行うことによって、ユーザにランダムデータを提示するための特別な仕組みを利用機 2502 に持たせることなく実現可能である点に特徴がある。

【0215】このように第 27 実施形態では、機密情報変換手段 2507 が都度生成するランダムデータを、UI 実行手段 2509 を通じて変換キーとしてユーザに提示し、ユーザから入力された仮の機密情報を同一の変換キーを用いて変換処理を行うことにより、ユーザからの直接入力される内容を毎回異なるものにすることが可能となる。仮の機密情報から真の機密情報が類推されることを防ぐ場合、毎回同じデータを与えるよりも乱数による異なるデータを与えた方がより機密性が高まるため、本実施形態がもたらすセキュリティ向上の実用的効果は大きい。

【0216】〔第 28 実施形態〕第 28 実施形態は前述した第 26 実施形態の機密情報保護に関する第 2 の変形例であり、IC カードシステムの構成及び処理の流れは第 26 および第 27 実施形態と基本的に同様である。この例は、図 26 に示したステップ 2601 において、もしくはステップ 2601 に先立って、ユーザが真の機密情報を誤って入力しないための注意メッセージを UI 実行手段 2509 がユーザに提示する点異なる。この注意メッセージの提示も、第 27 実施形態と同様に、第 9 ～ 第 25 実施形態で示した UI 情報の形成方法を用いてプロキシ装置 2503 が行うことができる。

【0217】図 29 は UI 実行結果として利用機上に表示される UI 画面とそこに情報を入力した状態の具体例を示す動作説明図である。この場合、利用機 2502 の UI 実行手段 2509 によってパスワード入力に関する情報がユーザに提示され、それを受けてユーザが仮の機密情報である仮パスワードを入力する。パスワードを入力する UI 部品には、パスワード入力領域、変換キー表示領域に付随して、誤って真の機密情報即ちリモートホスト 2504 の機密情報要求手段 2511 が要求する本当のアクセスパスワード（正パスワード）を入力しないよう、ユーザに注意を促すメッセージを追加している。なお、本実施形態では第 27 実施形態に倣う形で変換キーを表示しているが、第 26 実施形態に倣う形として変換キーを表示せず、注意メッセージのみを付加しても良い。

【0218】このように第 28 実施形態では、UI 実行手段 2509 がユーザに注意メッセージを示すことにより、誤って真の機密情報を入力してしまい、機密を漏洩させてしまうトラブルを防ぐ効果を得ることができる。

【0219】〔第 29 実施形態〕図 30 は本発明の第 29 実施形態に係る IC カードシステムの構成を示すブ

ック図である。第 29 実施形態は、IC カード 3001、利用機 3002、リモートホスト 3006 と共に、計算機ネットワーク 3007 上に複数のプロキシ装置 3003 ～ 3005 を備えた例である。また、本実施形態では、IC カード 3001 はプロキシ選択手段 3008 を備える。プロキシ選択手段 3008 は、計算機ネットワーク 3007 上にある複数のプロキシ装置 3003、3004、及び 3005 の中から、予め定めた規則に従って一つを選択する。選択されたプロキシ装置は前述した第 1 ～ 第 28 実施形態のいずれかに示すプロキシ装置として動作する。

【0220】なお、本実施形態ではプロキシ装置の数を 3 つとしたが、この数は限定的ではなく、実施可能な範囲において制限はない。また、リモートホストも 1 つとしたが、複数のリモートホストが計算機ネットワーク上に存在しても良い。これは他の実施形態においても同様である。

【0221】この第 29 実施形態では、計算機ネットワーク 3007 上に複数のプロキシ装置を設置し、IC カード 3001 にプロキシ選択手段 3008 を備えることにより、複数のプロキシ装置を選択的に使用することが可能となり、負荷分散、パフォーマンス最適化及びフォールトトレランス（障害に対する寛容性）の面でその実用的効果は大きい。

【0222】〔第 30 実施形態〕第 30 実施形態は前述した第 29 実施形態のプロキシ装置選択に関する第 1 の例であり、IC カードシステムの構成は図 30 と同様である。第 30 実施形態では、IC カード 3001 において、プロキシ選択手段 3008 はプロキシデータのリストから逐次的にプロキシ装置の情報を読み取り、使用に適するものが発見でき次第それを選択する。図 31 にプロキシ選択手段の動作の概念図を例示する。プロキシ装置選択の際に、使用に適するか否かを判断する方法は様々考えられるが、例えば実際に利用機を通じて通信ができるかどうかを調べる方法、通信できた場合に、予め定めたレスポンスタイムを下回ることをさらに条件とする方法等が挙げられる。これにより、比較的単純なアルゴリズムでプロキシ装置を選択することができる。

【0223】〔第 31 実施形態〕第 31 実施形態は前述した第 29 実施形態のプロキシ装置選択に関する第 2 の例であり、IC カードシステムの構成は図 30 と同様である。第 31 実施形態では、IC カード 3001 において、プロキシ選択手段 3008 はプロキシデータのリストからランダムにプロキシ装置の情報を読み取り、第 30 実施形態と同様に、使用に適するものが発見でき次第それを選択する。図 32 にプロキシ選択手段の動作の概念図を例示する。これにより、より負荷分散性を高めたプロキシ装置選択が可能となる。

【0224】〔第 32 実施形態〕第 32 実施形態は前述した第 29 実施形態のプロキシ装置選択に関する第 3 の

例であり、ＩＣカードシステムの構成は図３０と同様である。第３２実施形態では、ＩＣカード３００１において、プロキシ選択手段３００８は利用機３００２と通信を行って問い合わせをし、最適なプロキシ装置を選択する。この場合、ＩＣカード３００１よりも高い計算能力を持つ利用機３００２のプロキシ選択処理手段を利用して処理を行うことにより、プロキシ装置選択に関してよりきめ細かく柔軟な最適解を得ることが可能となる。ただし、利用機３００２の信頼度が低い場合、最適なプロキシ装置を偽って選択されたり、不正なプロキシ装置を故意に選択される可能性もあるため、ＩＣカード３００１と選択されたプロキシ装置との間で適切な相互認証が求められる。少なくとも、ＩＣカード３００１によるプロキシ装置の厳格な認証は必要不可欠である。なお、他の実施形態においても、ＩＣカードとプロキシ装置間で相互認証を行うことが望ましい。

【０２２５】〔第３３実施形態〕第３３実施形態は前述した第２９実施形態のプロキシ装置選択に関する第４の例であり、ＩＣカードシステムの構成は図３０と同様である。第３３実施形態では、第２９実施形態を基本として、図３３に示すようにさらにＩＣカード３００１のプロキシ選択手段３００８が持つプロキシ装置のリストを、ＩＣカードのユーザが追加、変更、削除することができるプロキシ情報操作手段３００９を備える。プロキシ情報操作手段３００９を用いた操作方法の例としては、利用機を通じてプロキシ情報の追加、変更、削除等を行う方法が挙げられるが、その際信頼度の高い利用機を用いることが望ましい。

【０２２６】これにより、ＩＣカードのユーザはプロキシ装置のリストを柔軟に操作することができ、新規のプロキシ装置の追加、プロキシ装置の変更や撤廃等に対して適切な対応を取ることが可能となり、その実用的効果は大きい。

【０２２７】〔第３４実施形態〕図３４は本発明の第３４実施形態に係るＩＣカードシステムの構成を示すブロック図である。第３４実施形態は、第１実施形態と同様に、ＩＣカード３４０１、利用機３４０２、プロキシ装置３４０３、リモートホスト３４０４を有して構成され、利用機３４０２とプロキシ装置３４０３、及びプロキシ装置３４０３とリモートホスト３４０４はそれぞれ計算機ネットワーク３４０５を介して接続される。利用機３４０２はＩＣカードリーダライタ３４０６を具備している。これら各構成装置の基本的な構成と関係は図１の第１実施形態と同様である。

【０２２８】本実施形態では、ＩＣカード３４０１はインセンティブ発行手段３４０７を、利用機３４０２はインセンティブ獲得手段３４０８をそれぞれ備える。インセンティブ発行手段３４０７は、インセンティブ獲得手段３４０８と通信を行い、利用機及び利用機の所有者や運用者が金銭的、事業的に有利となる状態をもたらすも

のである。インセンティブを授受する方法の例として、ＩＣカード３４０１が持っている有価値情報（例えば金銭と同等または類似の情報、ユーザの個人情報や利用度数情報など）を利用機３４０２に渡す、あるいは利用機３４０２が持っている情報（例えば広告情報、優待情報など）をＩＣカード３４０１に渡し、それをＩＣカード３４０１のユーザが閲覧したり取得することで利用機３４０２の所有者、運用者が直接的、間接的な意義を得ることが考えられる。なお、ＩＣカードのユーザ側においても何らかの利益を得るような仕組みについても適宜利用可能である。これにより、利用機３３０２を設置、運用する人間あるいは組織に対してその見返りを与えることが可能となり、その実用的効果は大きい。

【０２２９】〔第３５実施形態〕第３５実施形態は前述した第３４実施形態のインセンティブ授受に関する第１の例であり、ＩＣカードシステムの構成は図３４と同様である。第３５実施形態では、インセンティブとして商業広告を用いる。即ち、ＩＣカード３４０１のインセンティブ発行手段３４０７は、利用機３４０２のインセンティブ獲得手段３４０８から、商業広告に関わる情報を受け取る。そして、ＩＣカード３４０１のユーザがこの情報を見ることにより商業広告効果が生じ、利用機３４０２の所有者もしくは運用者が、直接的もしくは間接的に商業広告収入を得ることが可能となる。

【０２３０】〔第３６実施形態〕第３６実施形態は前述した第３４実施形態のインセンティブ授受に関する第２の例であり、ＩＣカードシステムの構成は図３４と同様である。第３６実施形態では、インセンティブとして金銭もしくはその他の有価値情報を用いる。例えば金銭を用いた場合は、ＩＣカード３４０１のインセンティブ発行手段３４０７は、利用機３４０２のインセンティブ獲得手段３４０８に対し電子化された情報の授受により金銭支払いを行う。金銭以外の有価値物についても同様である。これにより、利用機３４０２の所有者もしくは運用者は、より直接的な利益を得ることが可能となる。

【０２３１】〔その他の実施形態〕本発明に係るＩＣカードシステムは、上述した実施形態に限定されるものではなく、構成や手順に関して種々の追加、変更が可能である。以下にその他の実施形態としていくつかの例を示す。

【０２３２】上述の第１～第３６実施形態において、構成装置であるＩＣカードを、ＩＣカードに類似したアーキテクチャを持つＩＣタグに置き換えた構成とすることも可能である。ＩＣタグは演算処理及び利用機との通信を行うことができる点においてＩＣカードに類似するが、その外形特徴はボタン型、札型、シール型、もしくは装身具に埋め込んだもの等、様々な形態にて実施し得る。

【０２３３】また、上述の実施形態において、構成装置であるＩＣカードを、携帯電話を含む携帯型情報端末に

10

20

30

40

50

置き換えた構成とすることも可能である。ただし、携帯型情報端末は電波、赤外線、接触端子等の手段を用いて利用機と直接通信を行うことが可能であることが条件である。

【0234】また、上述の実施形態において、構成装置である IC カードを、マイコン内蔵メモリカードに置き換えた構成とすることも可能である。マイコン内蔵メモリカードは、比較的大容量の半導体メモリを持つカード型記憶媒体に、IC カードと同様の処理能力と、利用機との通信機能とを付加した装置である。なお、大容量メモリカードと IC カードとを、他の機器で接続したものを

用いた場合でも同様に実施可能である。

【0235】さらに、上述の実施形態において、構成装置である利用機を、街頭、店舗、駅、公共施設、学校、図書館等の不特定多数の人間が訪れる場所に設置する公共端末を用いた構成とすることも可能である。このような利用機が設置された施設を訪れる人間は、これに対応する IC カードを持参することで本発明が示す種々のサービスを楽しむことができる。

【0236】また、上述の実施形態において、構成装置である利用機を、遊園地、博物館、イベント施設等の不特定多数の人間が訪れる場所で、レンタル品として貸し出される携帯電話機もしくは携帯型情報通信端末を用いた構成とすることも可能である。これにより、このような利用機を貸し出す施設を訪れる人間は、これに対応する IC カードを持参することで本発明が示す種々のサービスを楽しむことができる。

【0237】また、上述の実施形態において、構成装置である利用機を、レンタカーに備え付けられるカーナビゲーション装置（自車の現在位置を地図上に表示したり、目的地までの道案内をする装置）を用いた構成とすることも可能である。なお、レンタカーに備え付けのものではなく、カーナビゲーション装置単体のレンタルでも良い。このようなカーナビゲーション装置の貸し出しを利用する人間は、これに対応する IC カードを持参することで本発明が示す種々のサービスを楽しむことができる。

#### 【0238】

【発明の効果】以上説明したように本発明によれば、第 1 に、IC カード装置（IC カード）とリモートホストとの間に設けられて両者とデータ通信を行い、IC カード装置の代理として計算機ネットワーク上で機能するプロキシ装置（代理装置）を備え、さらにカード端末装置（利用機）が未知の変換アルゴリズムもしくは変換パラメータを用いてデータ変換を行うデータ変換手段を備えたことにより、IC カードがプロキシ装置に渡したデータを、IC カードユーザの意図通りに、かつ利用機ユーザにその結果を知られることなく、プロキシ装置内部において異なるデータに変化させることができる効果が得られる。

【0239】第 2 に、IC カード装置内のアプリケーシ

ョンがアクセスしようとするリモートホストのネットワーク上の位置及び通信方法に関わる情報を、プロキシ装置のデータ変換手段で生成したことにより、カード端末装置に対してアクセス先を隠蔽することができる効果が得られる。

【0240】第 3 に、IC カード装置とプロキシ装置の二者間で暗号化に関するアルゴリズムと鍵情報を予め取り決め、この取り決めに基づいてカード端末装置に内容を知られることなく任意の情報をやりとりするセキュアパスを設けたことにより、IC カード装置とプロキシ装置が通信する際に、中間に位置するカード端末装置に通信内容を隠蔽することができる効果が得られる。

【0241】第 4 に、上記セキュアパスを介して IC カード装置内におけるデータの暗号化手段を、アクセス先情報と転送データ情報について個別に備えたことにより、IC カード装置がリモートホストに引き渡す転送データの内容を、カード端末装置だけでなくプロキシ装置にも隠蔽することができる効果が得られる。

【0242】第 5 に、IC カード装置には UI リクエスト情報送信手段を備え、プロキシ装置に UI リクエスト情報受信手段と UI 情報送信手段を備え、カード端末装置に UI 情報受信手段と UI 実行手段を備えたことにより、カード端末装置が持たないフォントの文字列情報等を表示することができる効果が得られる。

【0243】第 6 に、UI 情報としてカード端末装置上に予め設けられた動作環境に適合するプログラムを用いたことにより、IC カード装置が想定する UI が、カード端末装置の構成や仕様に強く依存せず独自のものとして実現可能となる効果が得られる。

【0244】第 7 に、IC カード装置とプロキシ装置のどちらか片方もしくは両方に、カード端末装置の認証手段と評価手段を備えたことにより、IC カード装置もしくはプロキシ装置が、カード端末装置の信頼度情報を獲得することができる効果が得られる。

【0245】第 8 に、IC カード装置とプロキシ装置の両方にカード端末装置の評価手段を備え、片方が得た評価結果をセキュアパスを通じて他方に渡すようにしたことにより、IC カード装置もしくはプロキシ装置のいずれか片方がカード端末装置の信頼度を獲得できた場合、もう一方にその情報を渡すことができる効果が得られる。また、両方が個別にカード端末装置の信頼度を獲得した場合は、それぞれの評価結果を違いに確認し合うことにより信頼度評価をより確実に行うことができる効果が得られる。

【0246】第 9 に、IC カード装置に送信情報制御手段を備えたことにより、IC カード装置からカード端末装置に送信する情報内容をカード端末装置の信頼度に従って異なるものにすることができる効果が得られる。さらに、IC カード装置が機密情報として保持する情報をカード端末装置に送信しないよう送信情報制御手段を作



用させることにより、個人情報等をカード端末装置毎の信頼度に応じて管理することができる効果が得られる。

【0247】第10に、プロキシ装置に送信情報制御手段を備えたことにより、プロキシ装置からカード端末装置に送信する情報内容を、上記のICカード装置の場合と同様にカード端末装置の信頼度によって異なるものにでき、信頼度の低いカード端末装置には機密情報を渡さないといったセキュリティ管理を行うことができる効果が得られる。

【0248】第11に、プロキシ装置上において、上記のUI情報送信手段に、上記の送信情報制御手段を連動させ、カード端末装置の評価結果に従ってプロキシ装置からカード端末装置に送信するUI情報に対して変更、削除、追加等の処理を行うようにしたことにより、信頼度の低いカード端末装置を使用する場合、機密情報をカード端末装置の画面上に表示してそれを取得されて漏洩してしまったり、また暗証番号等を不用意に入力して取得されてしまうなどのトラブルを防止することができる効果が得られる。

【0249】第12に、ICカード装置もしくはプロキシ装置に機密情報変換手段を設け、ユーザがカード端末装置に入力した仮の機密情報を、機密情報変換手段が真の機密情報に変換することで、暗証番号、パスワード等の機密情報をカード端末装置に秘匿した状態でリモートホストに渡し、リモートホストのサービスを受けられるようになる効果が得られる。

【0250】第13に、ICカード装置にプロキシ選択手段を備えたことにより、ICカード装置毎、カード端末装置毎に持つ条件に従って異なるプロキシ装置が利用可能となり、ネットワーク負荷及びプロキシの処理負荷の集中緩和を図ることができる効果が得られる。

【0251】第14に、ICカード装置にインセンティブ発行手段を備え、カード端末装置にインセンティブ獲得手段を備えたことにより、カード端末装置の所有者、運営者が直接的もしくは間接的利益を獲得することができる効果が得られる。

#### 【図面の簡単な説明】

【図1】本発明の第1実施形態に係るICカードシステムの構成を示すブロック図。

【図2】本発明の第2実施形態に係るICカードシステムの構成を示すブロック図。

【図3】第2実施形態におけるアクセス先情報及び通信キーデータの関係を例示した動作説明図。

【図4】第2実施形態におけるアクセス先秘匿処理の流れを示したフローチャート。

【図5】本発明の第3実施形態に係るICカードシステムの構成を示すブロック図。

【図6】本発明の第5実施形態に係るICカードシステムの構成を示すブロック図。

【図7】本発明の第9実施形態に係るICカードシステ

ムの構成を示すブロック図。

【図8】第9実施形態におけるUI制御処理の流れを示したフローチャート。

【図9】第9実施形態のICカードシステムにおけるUIリクエスト情報及びUI情報のデータ構造、並びにUI実行結果の一例を示す動作説明図。

【図10】本発明の第13実施形態に係るICカードシステムの構成を示すブロック図。

【図11】第13実施形態における利用機の信頼度評価処理の流れを示したフローチャート。

【図12】本発明の第14実施形態に係るICカードシステムの構成を示すブロック図。

【図13】第14実施形態における利用機の信頼度評価処理の流れを示したフローチャート。

【図14】本発明の第16実施形態に係るICカードシステムの構成を示すブロック図。

【図15】本発明の第20実施形態に係るICカードシステムの構成を示すブロック図。

【図16】本発明の第24実施形態に係るICカードシステムの構成を示すブロック図。

【図17】第24実施形態におけるUI実行処理の流れを示したフローチャート。

【図18】第24実施形態におけるUIリクエスト情報の一例を示す動作説明図。

【図19】第24実施形態におけるUI情報及びUI実行結果の第1の例を示す動作説明図。

【図20】第24実施形態におけるUI情報及びUI実行結果の第2の例を示す動作説明図。

【図21】第24実施形態におけるUI情報及びUI実行結果の第3の例を示す動作説明図。

【図22】本発明の第25実施形態にUIリクエスト情報及びUI実行結果の例を示す動作説明図。

【図23】第25実施形態におけるUI実行結果の具体例を示す動作説明図。

【図24】第25実施形態におけるUI実行結果の具体例を示す動作説明図。

【図25】本発明の第26実施形態に係るICカードシステムの構成を示すブロック図。

【図26】第26実施形態における機密情報保護処理の流れを示したフローチャート。

【図27】第26実施形態におけるUI実行結果とリモートホストに渡されるデータの具体例を示した動作説明図。

【図28】第27実施形態におけるUI実行結果の具体例を示す動作説明図。

【図29】第28実施形態におけるUI実行結果の具体例を示す動作説明図。

【図30】本発明の第29実施形態に係るICカードシステムの構成を示すブロック図。

【図31】本発明の第30実施形態に係るプロキシ選択



動作の概念を示す説明図。

【図32】本発明の第31実施形態に係るプロキシ選択動作の概念を示す説明図。

【図33】本発明の第33実施形態に係るプロキシ情報操作機能を有するICカードを示す説明図。

【図34】本発明の第34実施形態に係るICカードシステムの構成を示すブロック図。

【図35】従来のICカードシステムの構成例を示すブロック図。

【符号の説明】

101 ICカード

\* 102 利用機

103 プロキシ装置

104 リモートホスト

105 計算機ネットワーク

106 送信用データ保持手段

107 データ送信手段

108 ICカードリーダライタ

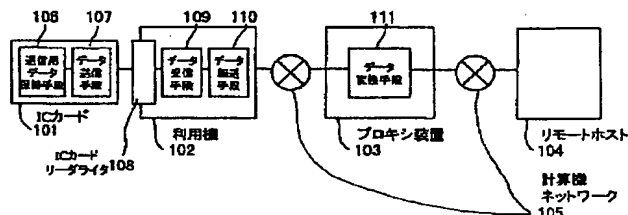
109 データ受信手段

110 データ転送手段

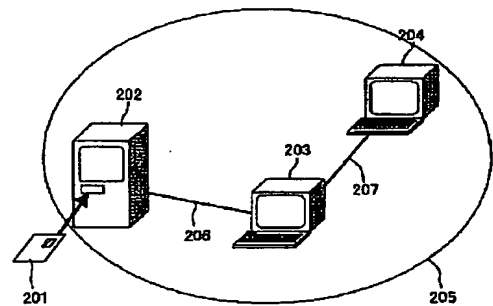
10 111 データ変換手段

\*

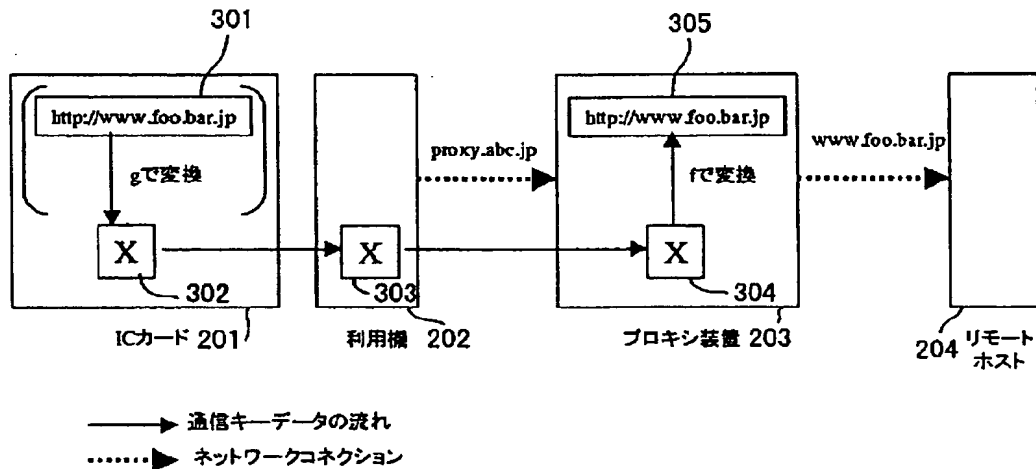
【図1】



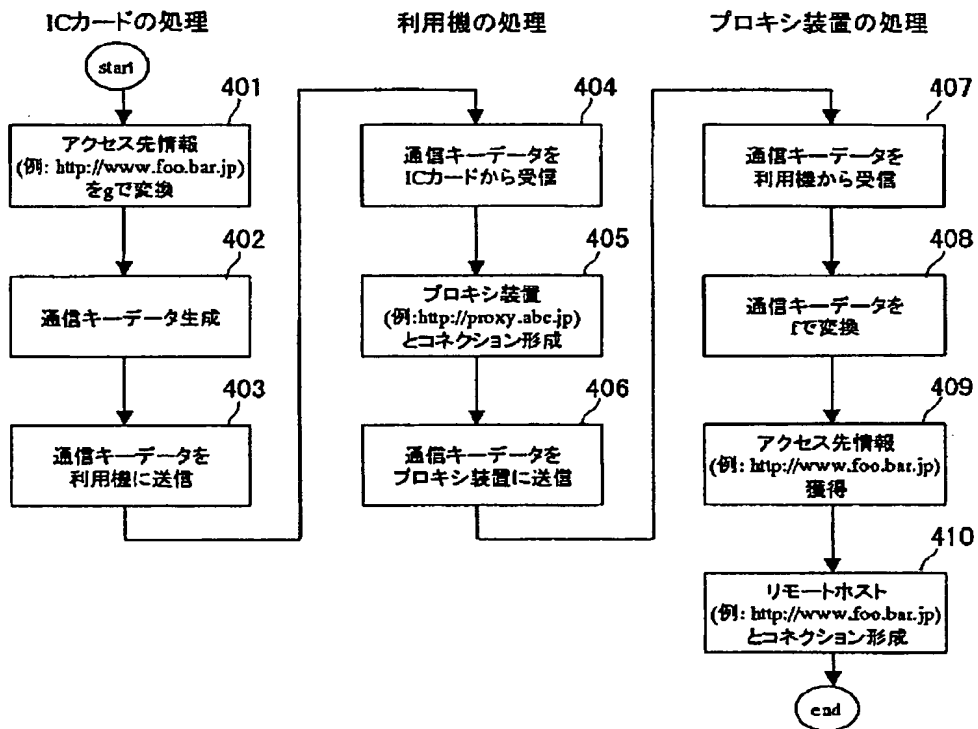
【図2】



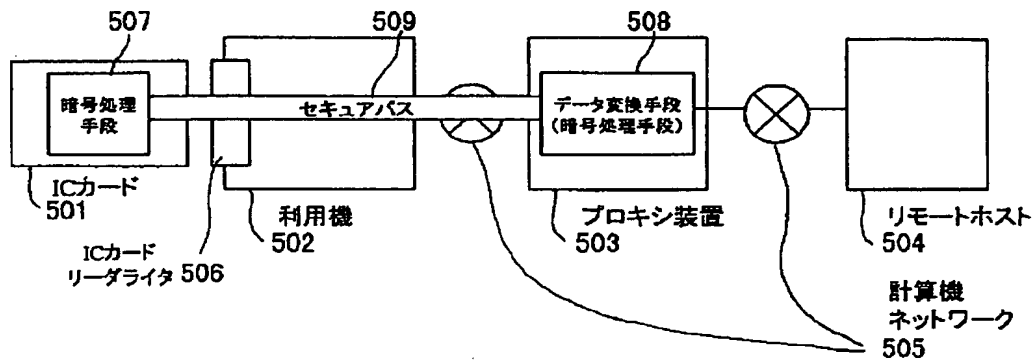
【図3】



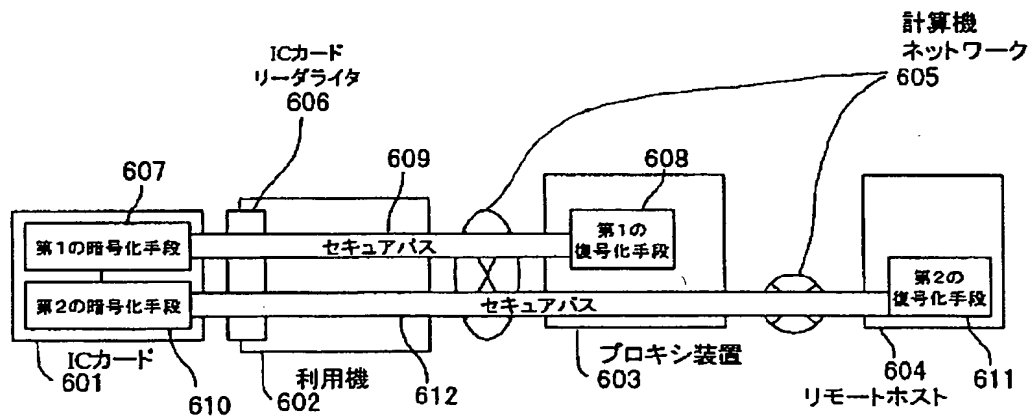
【図4】



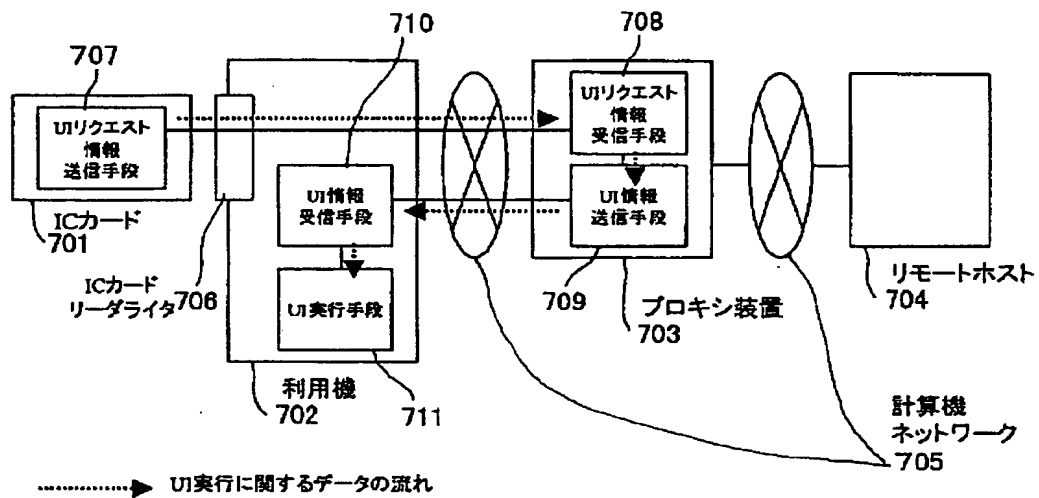
【図5】



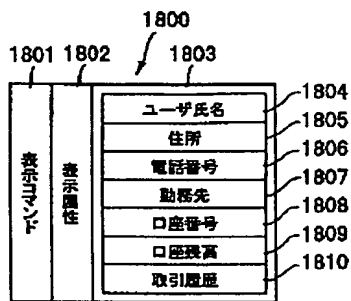
【図6】



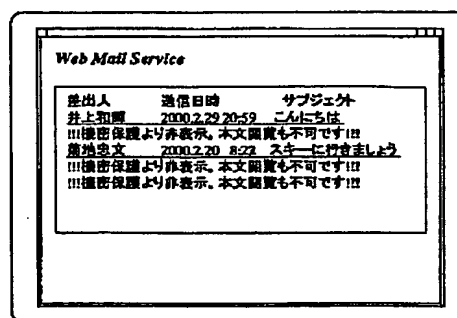
【図7】



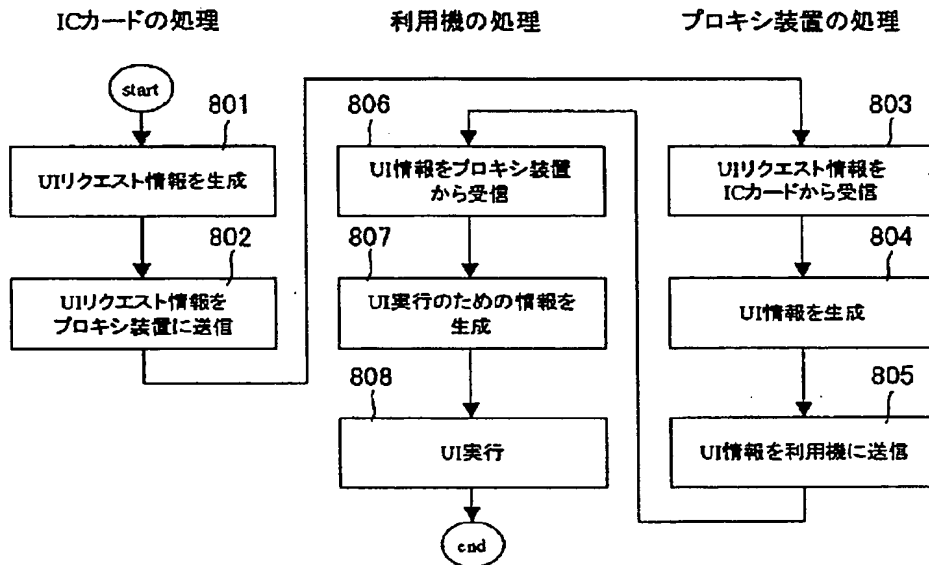
【図18】



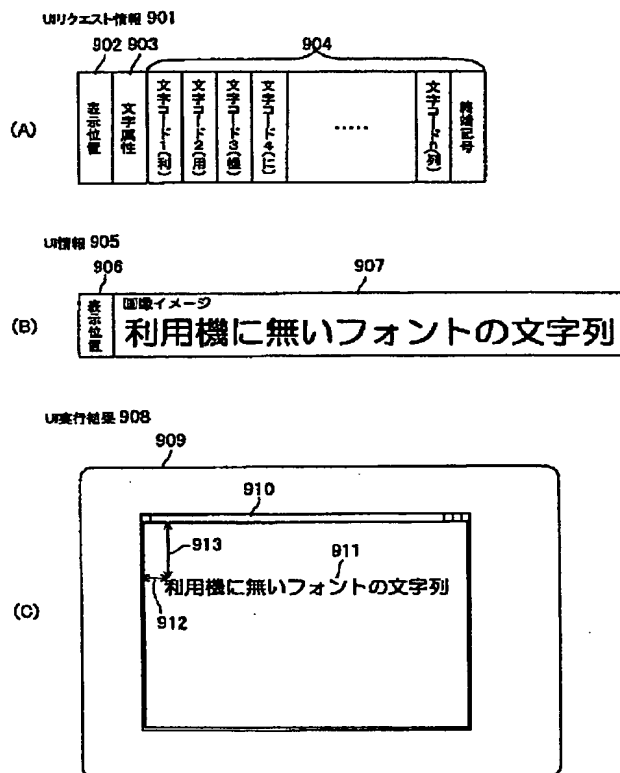
【図24】



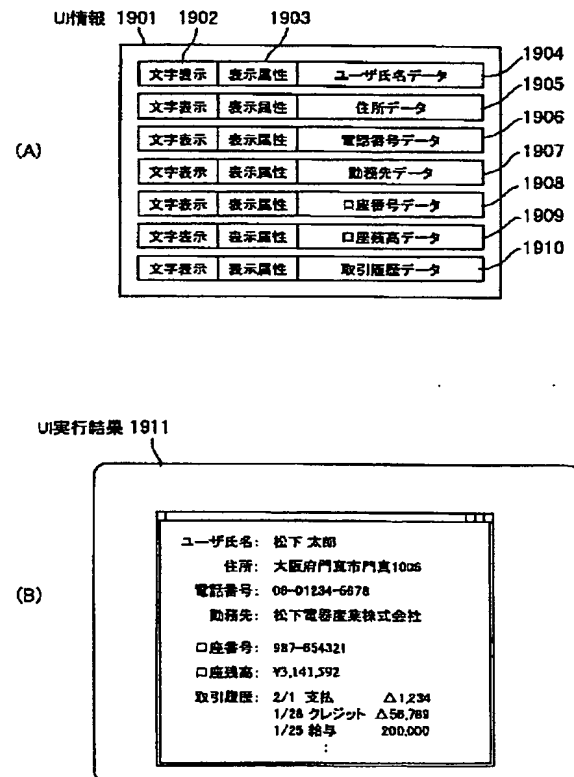
【図8】



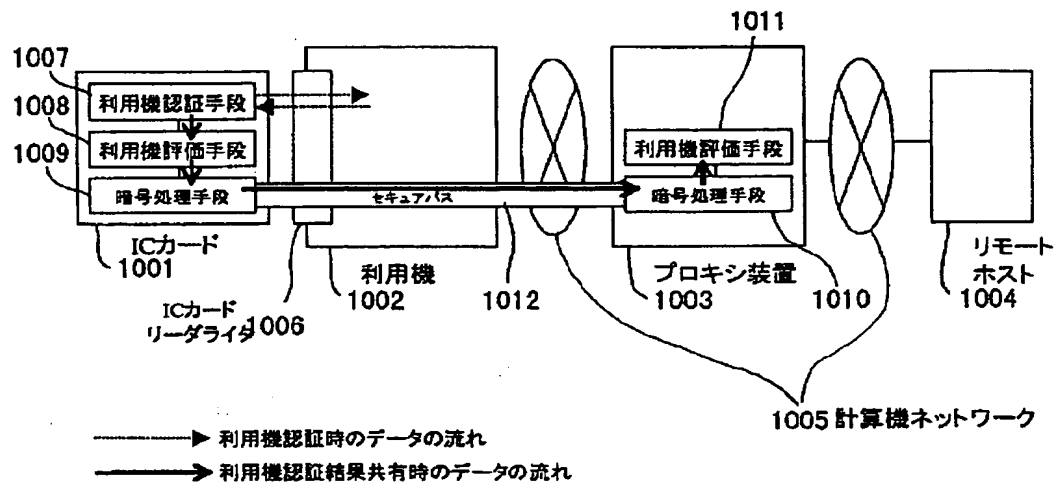
【図9】



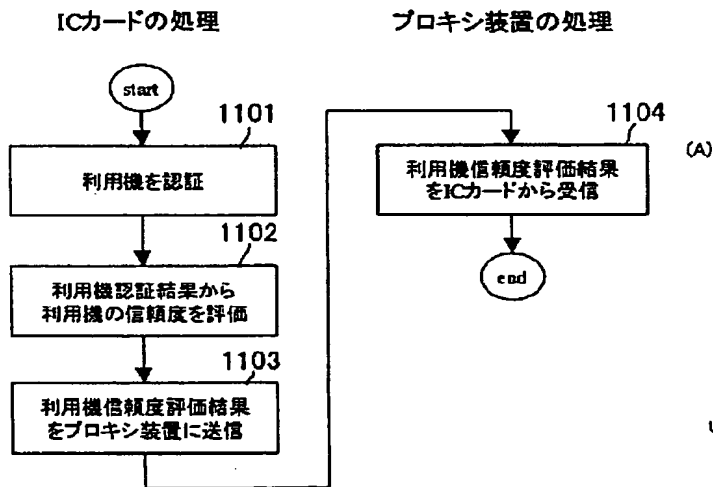
【図19】



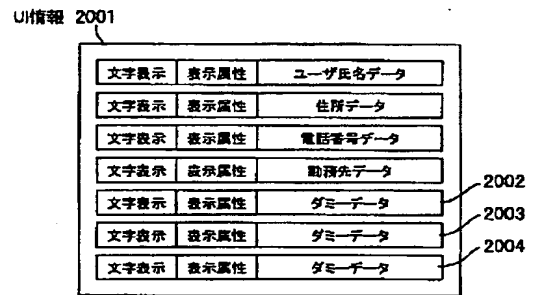
【図10】



【図11】

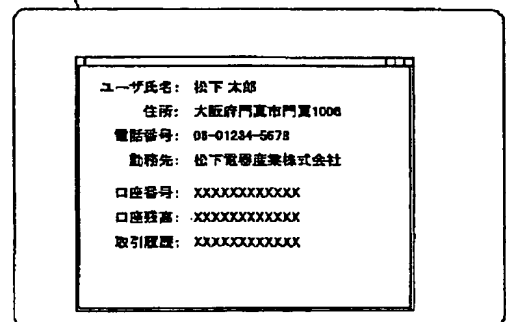


【図20】

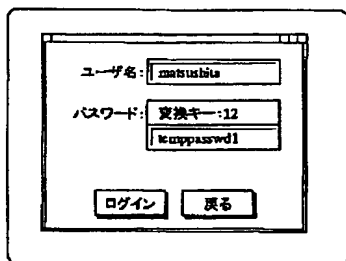


UI実行結果 2005

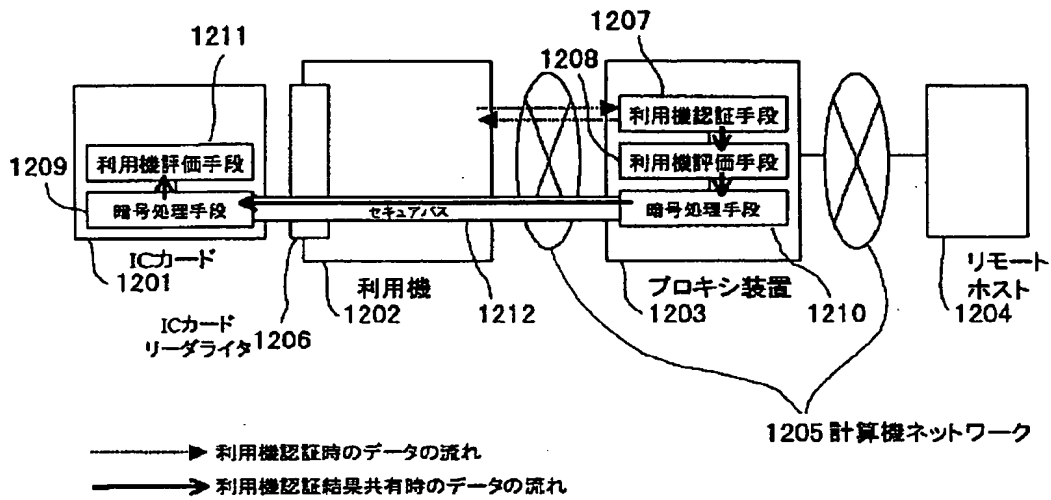
(B)



【図28】

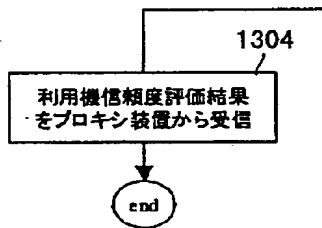


【図12】

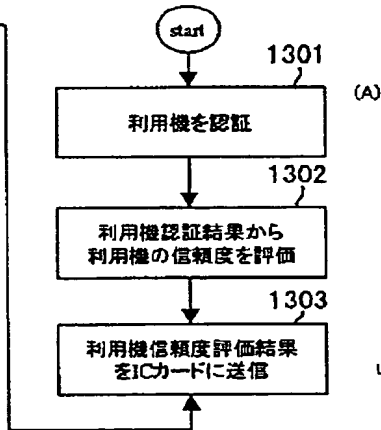


【図13】

ICカードの処理



プロキシ装置の処理



【図21】

UI情報 2101

文字表示	表示属性	ICカードユーザ氏名データ
文字表示	表示属性	ゲームデータ
文字表示	表示属性	ゲームデータ
文字表示	表示属性	ゲームデータ
文字表示	表示属性	ゲームデータ
文字表示	表示属性	ゲームデータ
文字表示	表示属性	ゲームデータ

UI実行結果 2102

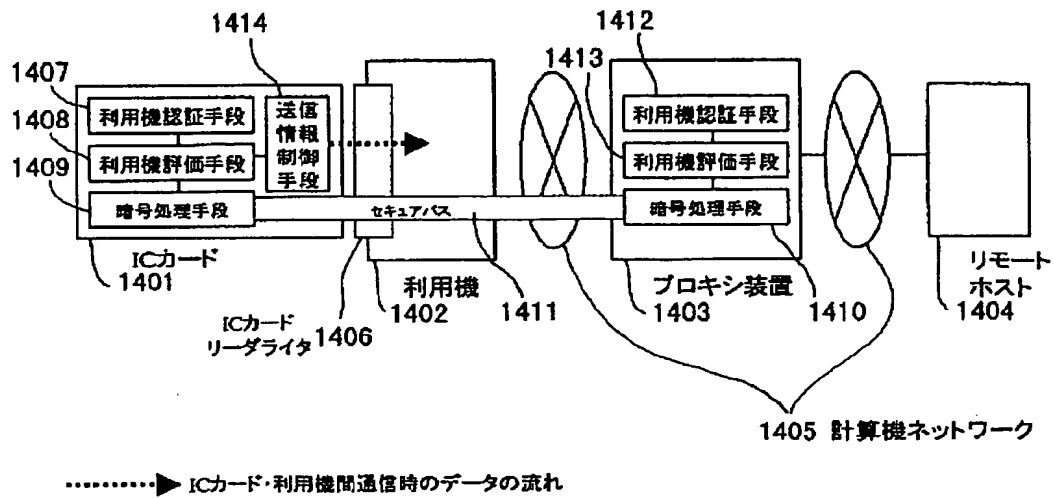
(B)

ユーザ氏名:	松本 太郎
住所:	XXXXXXXXXXXX
電話番号:	XXXXXXXXXXXX
勤務先:	XXXXXXXXXXXX
口座番号:	XXXXXXXXXXXX
口座種別:	XXXXXXXXXXXX
取引履歴:	XXXXXXXXXXXX

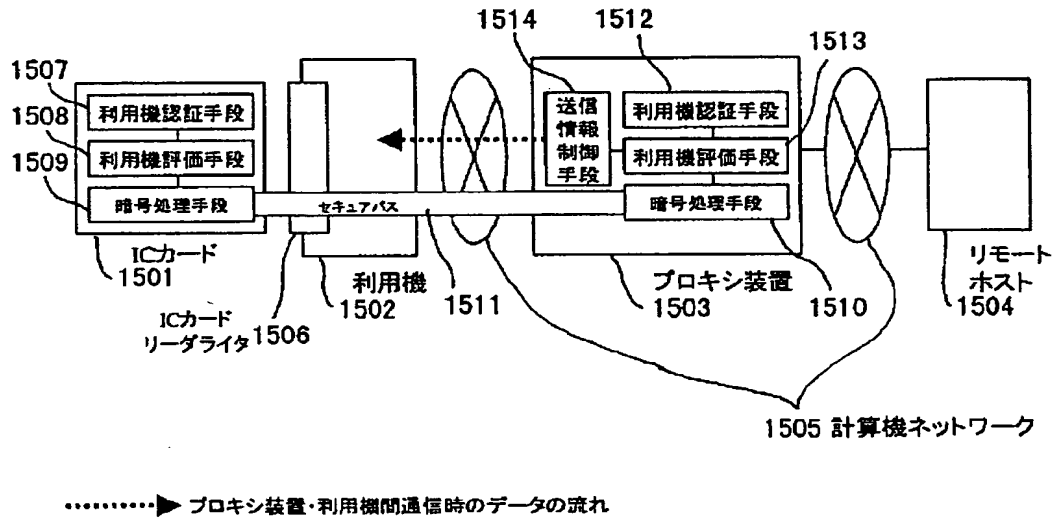
【図29】

ユーザ名:	mtsubu10
パスワード:	変換キー:12 tempasswd1
1度ここに本当のパスワードを入れないこと! 変換キーを見て仮のパスワードを入れて下さい。	
ログイン	戻る

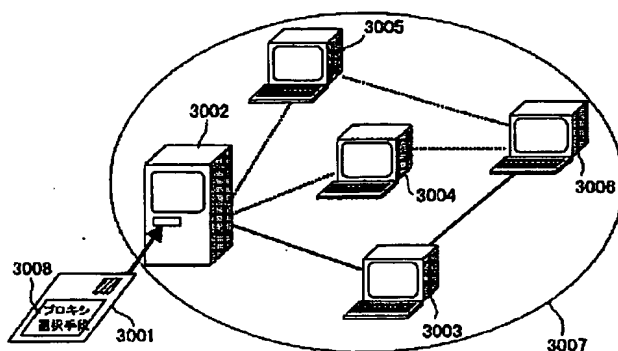
【図14】



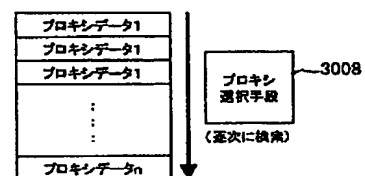
【図15】



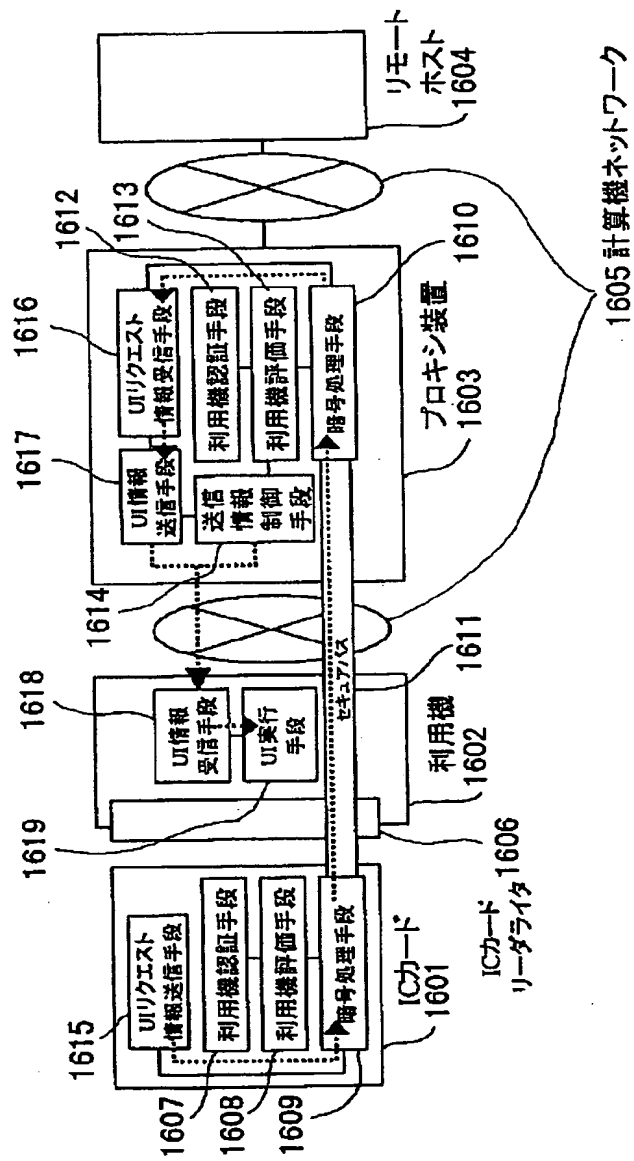
【図30】



【図31】



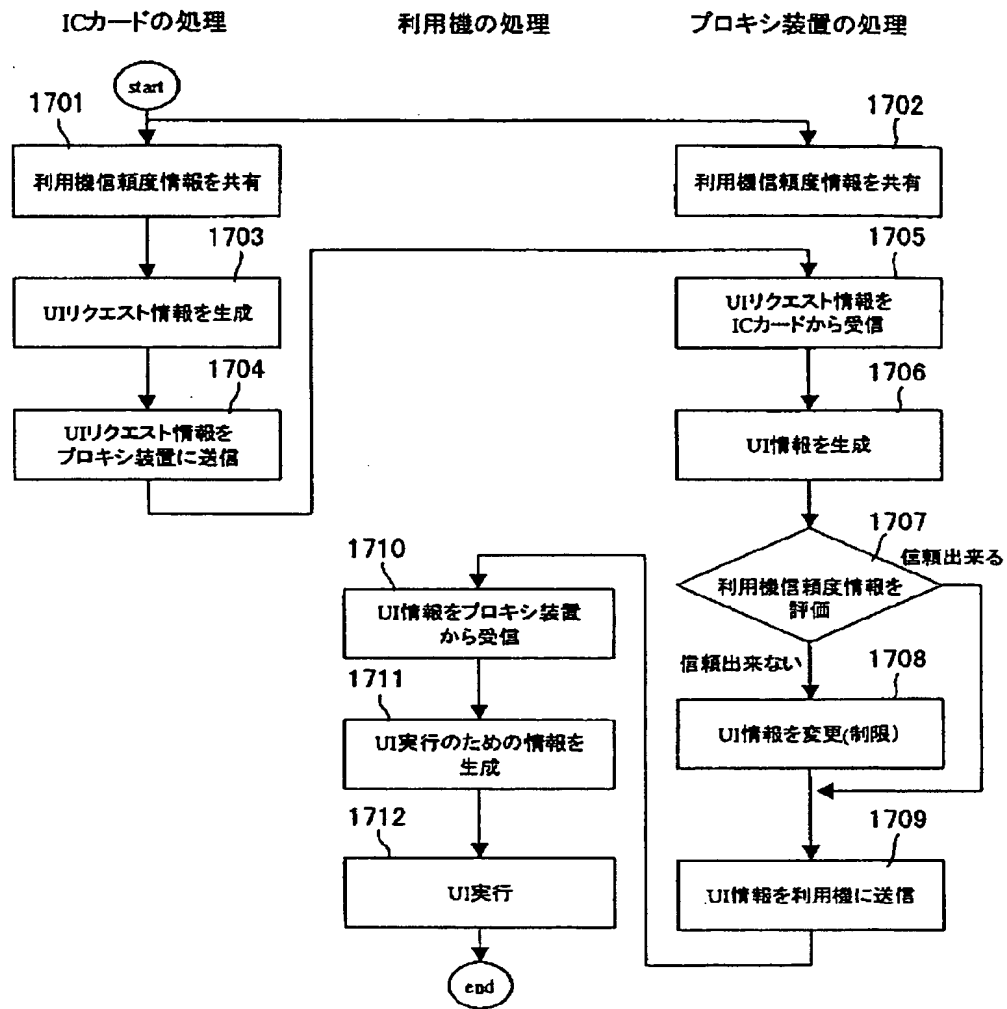
【図16】



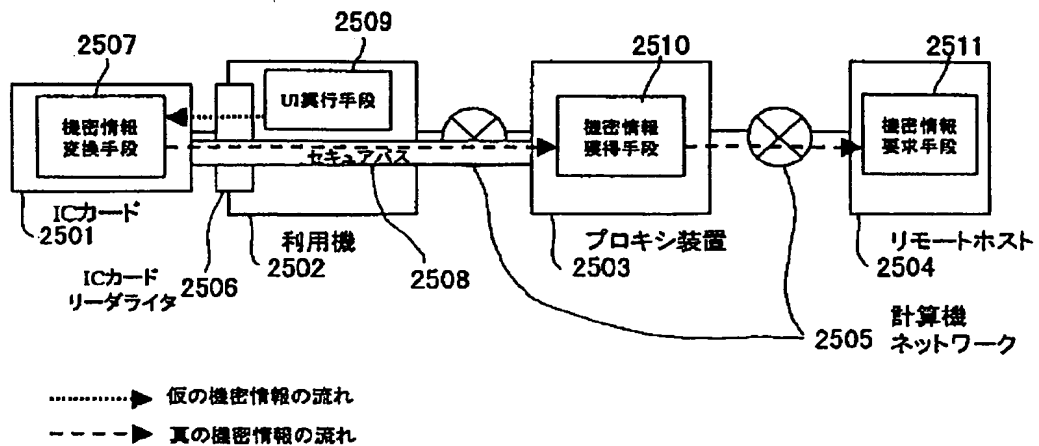
.....▶ UI実行に関するデータの流れ



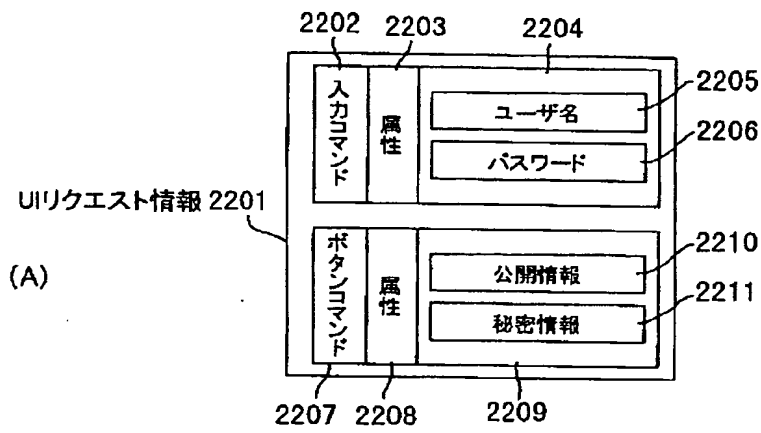
【図17】



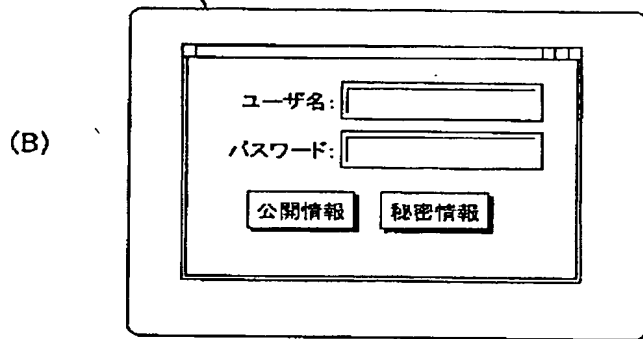
【図25】



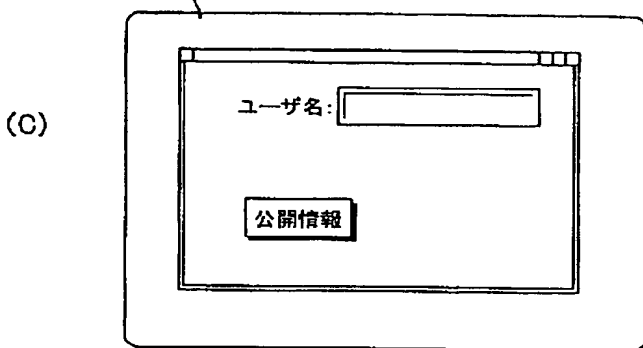
【図22】



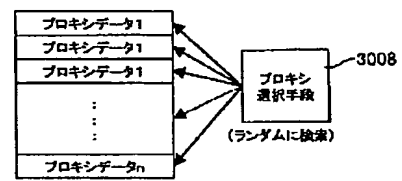
UI実行結果 2212



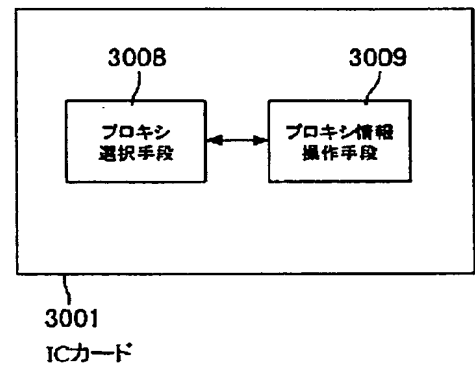
UI実行結果 2213



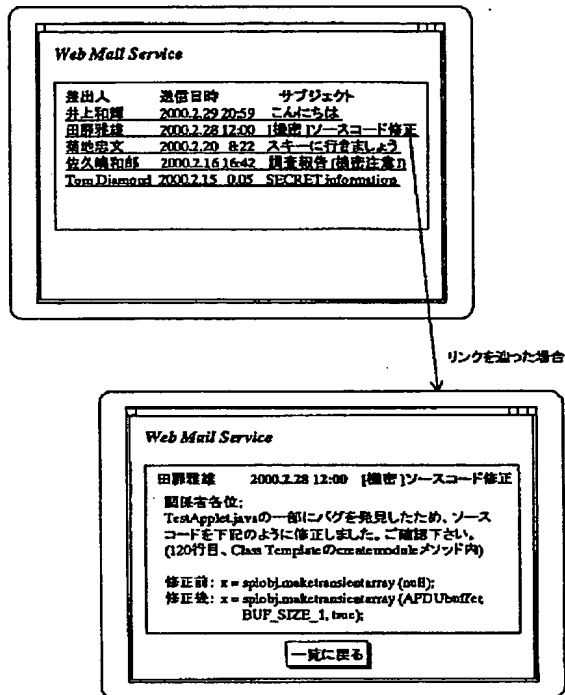
【図32】



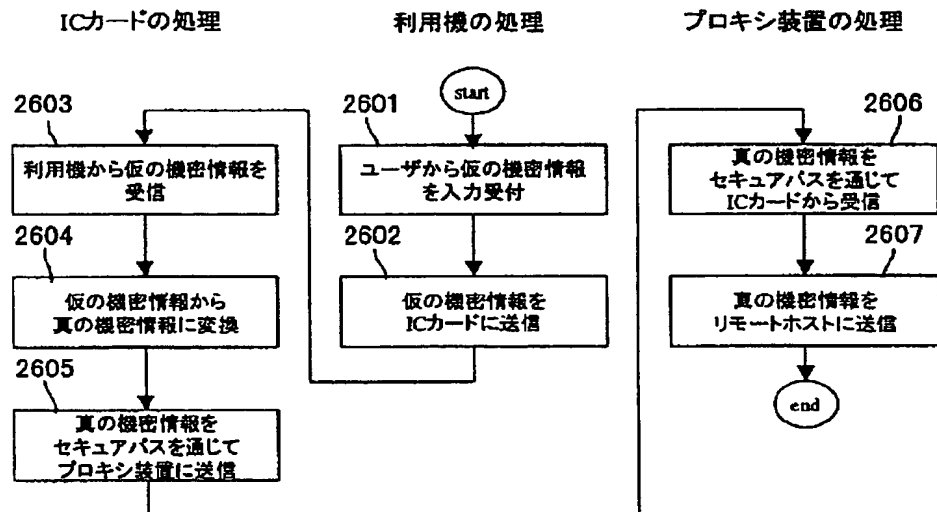
【図33】



【図23】

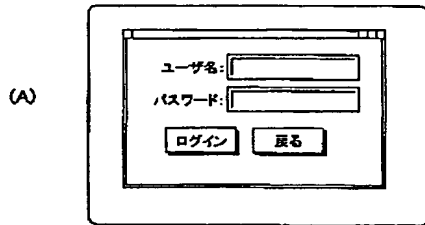


【図26】

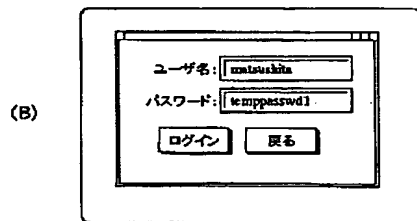


【図27】

利用機を通じてユーザに提示される画面例



ユーザが仮の機密情報として、文字列"tempasswd1"を入力した状態



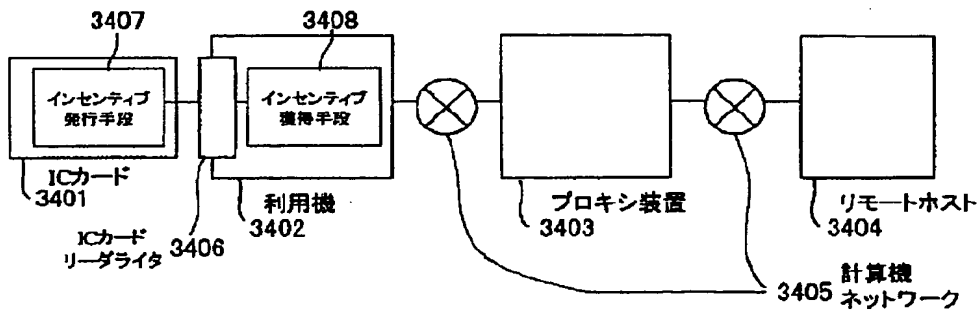
リモートホストに渡されるデータ

(C)

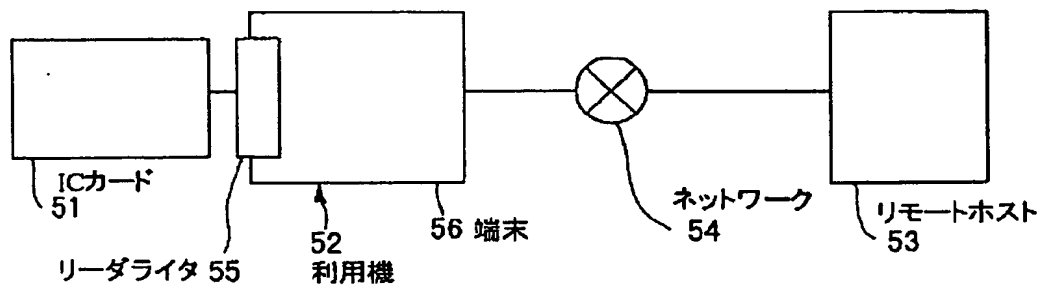
「ユーザ名」を示す識別子	文字列 "matsushita"
「パスワード」を示す識別子	文字列 "mYReALpassWORD"

※文字列 "mYReALpassWORD" は、文字列 "tempasswd1" から変換された真の機密情報である。

【図34】



【図35】



## フロントページの続き

(72)発明者 田藤 雅基  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72)発明者 菊地 隆文  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

F ターム(参考) 2C005 MB03 MB05 MB10 SA02 SA12  
SA25 TA27 TA28  
5B035 AA13 BB09 BC00 CA29  
5B058 CA23 KA02 KA04 YA20  
5B085 AE12 AE29  
5J104 AA01 NA02 NA35 NA37 NA40  
PA07